easy-solutions

Mumbai University Paper Solutions

Strictly as per the New Revised Syllabus (Rev - 2016) of
Mumbai University w.e.f. academic year 2018-2019
(As per Choice Based Credit and Grading System)

MU

COMPUTER NETWORKS

Semester V - Computer Engineering

Chapterwise Paper Solution upto May 2019.

TechKnowledge™ Publications

Scanned by CamScanner

easy - solutions

Mumbai

Computer Networks

Semester V - Computer Engineering

Strictly as per New Choice Based Credit and Grading System Syllabus
(Revise 2016) of Mumbai University with effective from Academic Year 2018-2019

TechKnowledge™ Publications

EM045A Price ₹ 75/-

Scanned by CamScanner

Computer Networks

(Semester V – Computer Engineering) (MU)

Copyright © TechKnowledge Publications. All rights reserved. No part of this publication may be reproduced, copied, or stored in a retrieval system, distributed or transmitted in any form or by any means, including photocopy, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

This book is sold subject to the condition that it shall not, by the way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior written consent in any form of binding or cover other than which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above.

Edition 2019

This edition is for sale in India, Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Sri Lanka and designated countries in South-East Asia. Sale and purchase of this book outside of these countries is unauthorized by the publisher.

Printed at : 37/2, Ashtvinayak Industrial Estate, Near Pari Company,
Narhe, Pune, Maharashtra State India,
Pune – 411041

Published by

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner,
Pune - 411 009. Maharashtra State, India
Ph : 91-20-24221234, 91-20-24225678.
Email : info@techknowledgebooks.com,
Website : www.techknowledgebooks.com

(Book Code : EMO45A)

Scanned by CamScanner

INDEX

Table of Contents

❑❑❑

Scanned by CamScanner

Syllabus

Module 1

Introduction to Networking :

Introduction to computer network, network application, network software and hardware components (Interconnection networking devices), Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services. Reference models: Layer details of OSI, TCP/IP models. Communication between layer.

Module 2

Physical Layer :

Introduction to Communication System, digital Communication, Electromagnetic Spectrum, Guided Transmission Media : Twisted pair, Coaxial, Fiber optics. Unguided media (Wireless Transmission): Radio Waves, Microwave, Bluetooth, Infrared, Circuit and Packet Switching.

Module 3

Data Link Layer :

DLL Design Issues (Services, Framing, Error Control, Flow Control), Error Detection and Correction (Hamming Code, CRC, Checksum), Elementary Data Link protocols, Stop and Wait, Sliding Window (Go Back N, Selective Repeat), HDLC, Medium Access Control sublayer : Channel Allocation problem, Multiple access Protocol (Aloha, Carrier Sense Multiple Access (CSMA/CD), Local Area Networks - Ethernet (802.3)

Module 4

Network layer :

Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (classfull and classless), Subnetting, Supernetting design problems, IPv4 Protocol, Network Address Translation (NAT), Routing algorithms : Shortest Path (Dijkastra's), Link state routing, Distance Vector Routing, Protocols - ARP, RARP, ICMP, IGMP Congestion control algorithms : Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms.

Module 5

Transport Layer :

The Transport Service : Transport service primitives, Berkeley Sockets, Connection management (Handshake), UDP, TCP, TCP state transition, TCP timers, TCP Flow control (sliding Window), TCP Congestion Control: Slow Start.

Module 6

Application Layer :

DNS: Name Space, Resource Record and Types of Name Server. HTTP, SMTP, Telnet, FTP, DHCP.

□□□

Scanned by CamScanner

Computer Networks

Chapter 1 : Introduction to Networking

Q. 1 Compare ring and star network topologies. Dec. 15

Ans. :

Sr. No.	Ring	Star
1.	Media failure on uni-directional or single loop ring causes complete network failure.	Media faults are automatically isolated to the failed segment.
2.	Relatively difficult to reconfigure.	Relatively easy to configure.
3.	It is difficult to troubleshoot.	Easy to troubleshoot.
4.	The failure of one computer can affect the whole network.	The failure of single computer or cable doesn't bring the network down.
5.	No computer has a monopoly over the network.	Failure of the central hub causes the whole network failure.
6.	Adding and removing computers disrupts the network.	Adding and removing the computers is relatively easier.

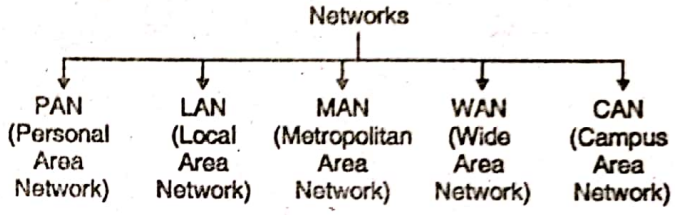
Q. 2 Compare bus and star network topologies. Dec. 15

Ans. :

Sr. No.	Bus	Star
1.	Uses a cable as bus or backbone to connect all nodes.	Uses a central hub to connect the nodes to each other.
2.	Baseband or broadband coaxial cable is used.	Twisted pair, coaxial cables or optical fiber cables are used.
3.	If a part of bus fails, the whole network fails.	Failure of the central hub will make the entire network collapse.
4.	Adding an new node is difficult.	Adding and removing a node is relatively easy.
5.	Fault diagnosis is relatively difficult.	Fault diagnosis is easy.

Q. 3 What are the different categories of the network classification ? Dec. 13

Ans. :



(G-1400) **Fig. 1.1 : Network categories**

Q. 4 Design a LAN network for your institute. May 05

Ans. :

The Local Area Network (LAN) is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings. LANs are very widely used in a variety of applications. LANs are easy to design and troubleshoot. The personal computers and workstations in the offices are interconnected via LAN. The exchange of information and sharing of resources becomes easy because of LAN.

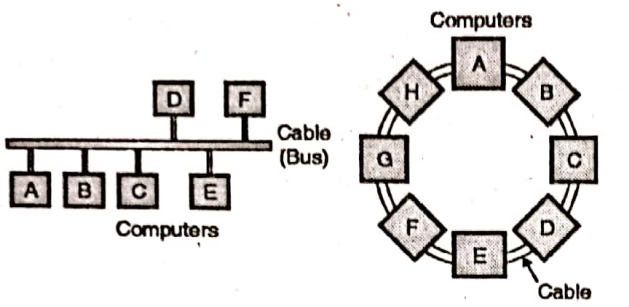
In LAN all the machines are connected to a single cable. Different types of topologies such as Bus, Ring, Star, Tree etc. are used for LANs. LAN uses a layered architecture and they are capable of operating at hundreds of Mbits/sec. A Local Area Network (LAN) is usually a privately owned and links the devices in a single office, building or campus of upto a few kilometres in size as shown in Fig. 1.1. Depending on the needs of an organisation and the type of technology used, a LAN can be as simple as a few computers and a printer at home or it can contain many computers in a company and include voice, sound and video peripherals.

LANs are widely used to allow resources to be shared between personal computers or workstations. The resources to be shared can be hardware like a printer or softwares or data. In a LAN one of the computer can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients. LAN's are also distinguished from MAN's and WAN's based on the transmission media they use and topology. In general a given LAN will use only one type of transmission medium. The most common networking topologies used are bus, ring and star. The data rates for LAN can now range from 10 Mbps to 16 Gbps.

Scanned by CamScanner

LAN topologies :

Various topologies are possible for the broadcast LANs such as bus topology or ring topology as shown in Fig. 1.1.



(a) Bus topology (b) Ring topology

(G-32)Fig. 1.1 : LAN topologies

Static and dynamic broadcast networks :

The broadcast networks are further classified into two types namely :

1. Static networks and 2. Dynamic networks.

This classification is based on how the common channel is allocated. In static allocation, each machine is allowed to broadcast only in its allotted time slot. But static allocation wastes the channel capacity when a machine does not want to transmit in its allotted time slot. Hence most of the systems try to allocate the channel dynamically i.e. on demand.

LAN components :

Some of the important LAN components are as follows :

1. Workstations.
2. File servers.
3. Gateway.
4. Network interfacing unit.
5. Active and passive hubs.
6. LAN cables or communication channels.

Workstation :

Workstation refers to the individual, single computer. A communication capability is added to enable it for networking.

File server :

File server is a computer that allows the sharing of data, software and hardware resources by running special softwares.

Gateway :

It assists the transfer of data from one LAN to the other LAN.

Network Interfacing Unit (NIU) :

It is a unit which consists of hardware as well as software. It uses microprocessor to control the access and communication in a network.

LAN cables or communication channel :

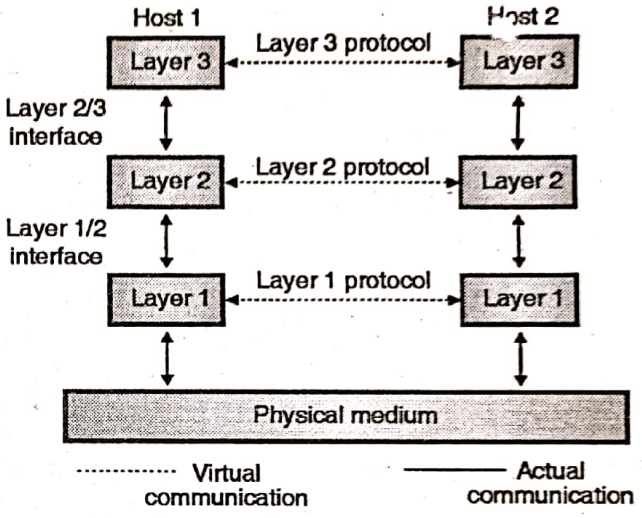
A cable is used for connecting the computers in a LAN. The communication from one computer to others takes place over the cables. So cables are called communication channels. The twisted pair, coaxial cables or optical fiber cables are used in LANs.

Q. 5 Explain the need of layered design for communication and networking.

May 05, Dec. 05, May 07, Dec. 09, May 12, May 13, Dec. 14, Dec. 17

Ans. :

Most networks are organized in the form of a series of layers or levels as shown in Fig. 1.2. To reduces the design complexity.



(G-49) Fig. 1.2 : Layers, protocols and interfaces

The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers. Layer n on one machine (source) will communicate with layer n on another machine (destination).

The rules and conventions used in this communication are collectively known as the layer "n" protocol. Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released. Violation of the protocol will lead to the communication difficulties or failure.

Peer :

A three layer network is shown in Fig. 1.2. The entities comprising the corresponding layers on different machines are called as **peers.** The communication actually takes place between the peers using the protocol. The dotted lines in Fig. 1.2 shows the virtual communication and physical communication is shown by solid lines.

Reasons for having Layered Protocols and its Benefits :

The process of establishing a link between two devices to communicate and share information is complicated. There are many functions which are to be taken into consideration to allow an effective communication to take place. To organize all these functions in an organized way the designers felt the need to develop network architecture.

Scanned by CamScanner

In the network architecture various tasks and functions are grouped into related and manageable sets called **LAYERS.** A network architecture can be defined as a set of protocols that tell how every layer is to function.

The reasons and advantages of using the network architecture are as follows :

1. It simplifies the design process as the functions of each layers and their interactions are well defined.
2. The layered architecture provides flexibility to modify and develop network services.
3. The number of layers, names of the layers, and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers some services to its upper layer.
4. The concept of layered architecture is a new way of looking at the networks.
5. Addition of new services and management of network infrastructure becomes easy.
6. Due to segmentation (layered structure), it is possible to break difficult problems into smaller and more manageable tasks.
7. Logical segmentation allows parallel working by different teams on different tasks simultaneously.

Q. 6 List design issues in OSI layers.

Dec. 10, May 13, May 15, Dec. 15, Dec. 16

Ans. :

Addressing :

For every layer, it is necessary to identify senders and receivers. Some mechanism needs to be used for the same. Since there are many possible destinations for a packet, some form of addressing is needed in order to specify a specific destination.

Error Control :

Another important issue is the error control because physical communication channels can introduce errors in the data travelling on them. Error detection and correction both are essential. Many error detecting and correcting codes are known out of which those which are agreed upon and receiver should be used. The receiver should be able to tell the sender by some means, that it has received a correct message or a wrong message.

Avoid Loss of Sequencing :

All the communication channels cannot preserve the order in which messages are sent on it. So there is a possibility of loss of sequencing. That means messages are not received serially at the receiver. To avoid this, all the packets of a message should be numbered so that they can be put back together at the receiver in the appropriate sequence.

Ability of Receiving Long Messages :

At several levels, one more problem needs to be solved, which is inability of all processes to accept arbitrarily long messages. So a mechanism needs to be developed to de-assemble (break into small messages), transmit and then reassemble messages.

To use Multiplexing and Demultiplexing :

Multiplexing and demultiplexing is to be used to share the same channel by many sources simultaneously. It can be used for any layer. Multiplexing is needed at the physical layer level.

Q. 7 Differentiate between the connectionless and connection oriented service.

Dec. 12, May 13, May 16

Ans. :

Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection needs to be established	Connection need not be established
6.	Delays	More	Less
7.	Overheads	Less	More
8.	Packets travel	Sequentially	Randomly
9.	Congestion due to overloading	Not possible	Very much possible

Q. 8 What is ISO-OSI reference model ? May 17

Ans. :

An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.

Q. 9 Describe OSI reference model with a neat diagram.

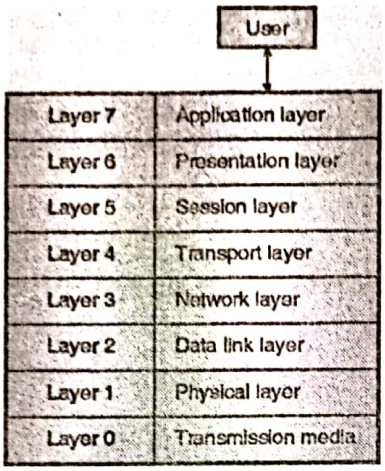
Dec. 03, Dec. 07, May 10, May 11, Dec. 12, May 15

Ans. : The users of a computer network are located over a wide physical range i.e. all over the world. Therefore to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed. These standards will fit into a framework which has been developed by the "International organization of standardization (ISO)".

This framework is called as "Model for open system interconnection (OSI)" and it is normally referred to as "OSI reference model". Fig. 1.3 shows the seven layer architecture of ISO-OSI reference model. It defines seven levels or layers in a complete communication system. The lowest layer is physical layer

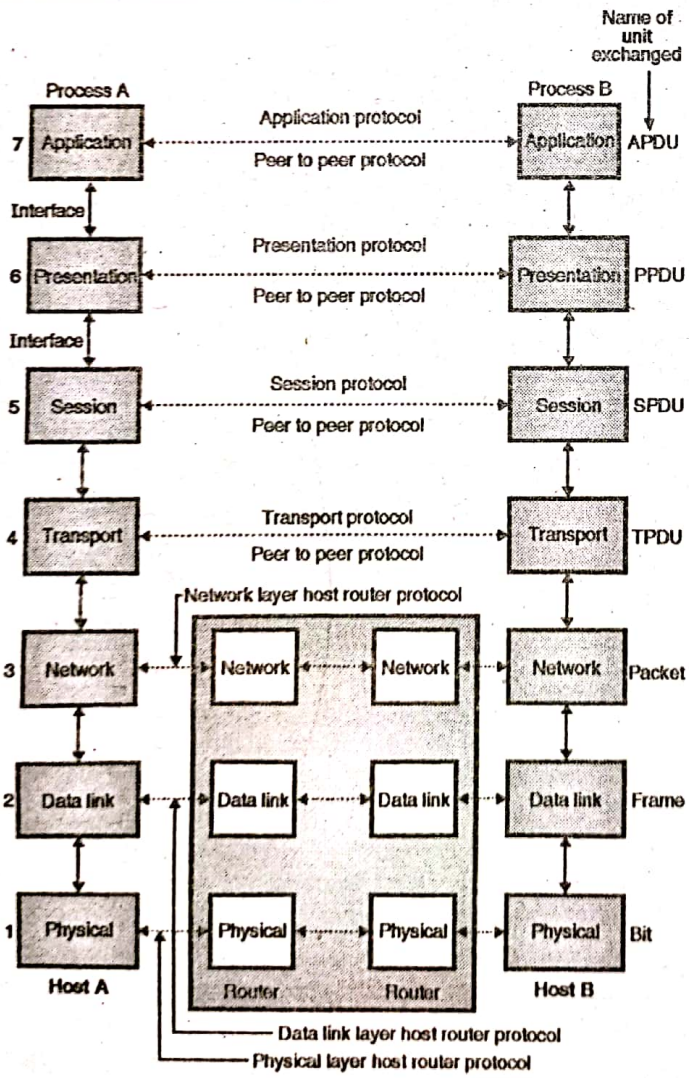
Scanned by CamScanner

and highest one is called as the application layer. A more detailed OSI reference model is shown in Fig. 1.3(a). The OSI model shown in Fig. 1.3(a) does not contain the physical medium.



(G-59) **Fig. 1.3 : A seven layer ISO-OSI reference model**

This model is based on a proposal developed by the International Standards Organization (ISO). It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e. the systems which are open for communication with other systems.



(G-60) **Fig. 1.3(a) : The OSI reference model**

Table 1.1 shows various layers and its functions.

Table 1.1 : Functions of the layers of ISO-OSI model

Level	Name of the layer	Functions
1.	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2.	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4.	Transport layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session management.
6.	Presentation layer	It works as a translating layer.
7.	Application layer	Retransferring files of information, LOGIN, password checking etc.

All the applications need not use all the seven layers shown in Fig. 1.3(a). The lower three layers are enough for most of the applications. Each layer is built from electronic circuits and/or software and has a separate existence from the remaining layers. Each layer is supposed to handle message or data from the layers which are immediately above or below it.

This is done by following the protocol rules. Thus each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

Q. 10 Which layer is used for the following :

1. **To route packets**
2. **To convert packets to frame**
3. **To detect and correct errors.**
4. **To run services like FTP, telnet etc.**

May 17

Scanned by CamScanner

Ans. :

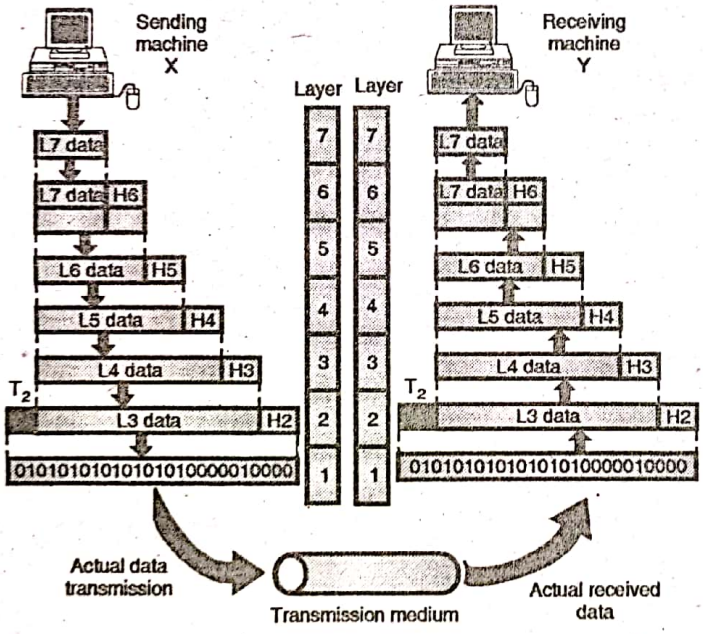
1. To route packets : Network layer
2. To convert packets to frame : Data link layer
3. To detect and correct errors : Data link layer
4. To run services like FTP, telnet etc. : Application layer

Q. 11 Explain how information is exchanged between two nodes using OSI model. Dec. 09

Ans. :

At the physical layer, communication is direct i.e. machine X sends a stream of bits to machine Y. At higher layers, each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it as shown in Fig. 1.4. The information added by each layer is in the form of headers or trailers. Headers are added to the message at the layers 6, 5, 4, 3, and 2. A trailer is added at layer 2.

At layer 1 the entire package is converted to a form that can be transferred to the receiving machine. At the receiving machine, the message is unwrapped layer by layer with each process receiving and removing the data meant for it.



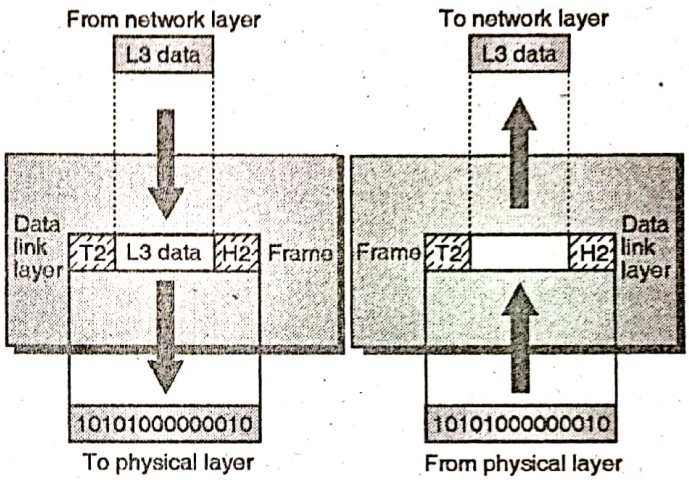
(G-61) **Fig. 1.4 : An exchange using the OSI model**

The upper OSI layers are always implemented in software (4, 5, 6 and 7) and lower layers are a combination of hardware and software (2, 3) except for the physical layer which is mostly hardware. Layers 1, 2 and 3 (i.e. physical , data link and network) are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing and transport timing and reliability. Layer 4, the transport layer ensures end to end reliable data transmission.

Q. 12 Layers 5, 6 and 7 (i.e. session, presentation and application) they allow interoperability among unrelated software systems. Write short notes on : Data Link Layer. May 10

Ans. :

It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown in Fig. 1.5.

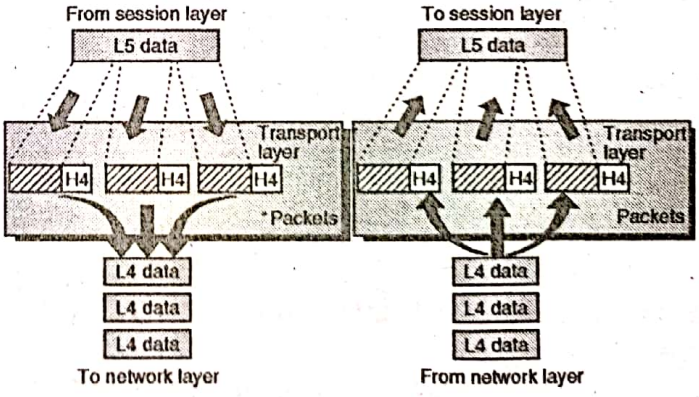


(G-63) **Fig. 1.5 : Data link layer**

Q. 13 Write short notes on : Transport Layer. May 10

Ans. :

The function of the transport layer is the process to process delivery of the entire message. It ensures that the whole message reaches the destination intact and in order, with both error control and flow control incorporated at the source and destination. Fig. 1.6 shows the relationship of the transport layer to the network layer and session layer.



(G-67) **Fig. 1.6 : Transport layer**

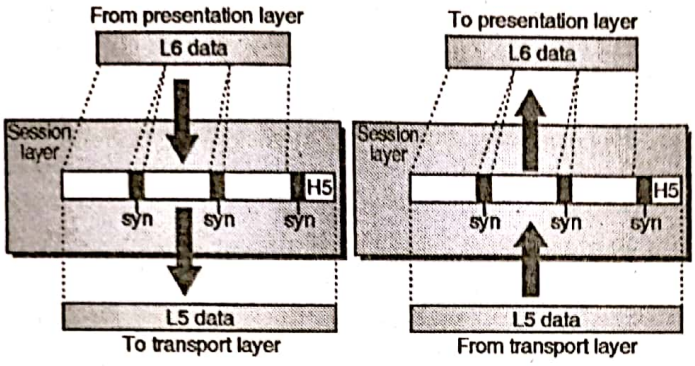
Q. 14 Explain how a session layer establishes, maintains and synchronises the interaction between two communicating hosts. May 04, May 15, Dec. 16

Ans. :

The main function of this layer is to establish, maintain and synchronise the communication between interested systems.

Scanned by CamScanner

Fig. 1.7 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) **Fig. 1.7 : Session layer**

The session layer performs the following functions :

It allows two systems to start a dialog. The communication between two processes will take place either in half duplex or full duplex mode. The other function of this layer is synchronization.

The session layer is not inherently concerned with security and the network logon process. The primary functions of this layer is exchange of messages between two interested systems called as **a dialog.**

Infact 22 different services are provided by the session layer. These are grouped into subsets such as the Kernel Function Unit, the Basic Activity Subset and the Basic Synchronization Subset. However the two most important services provided by the session layer are :

1. Dialog control and 2. Dialog separation

1. Dialog control :

Dialog control is the means by which a sending and receiving systems initiate a dialog, exchange messages and finally end the dialog.

2. Dialog separation :

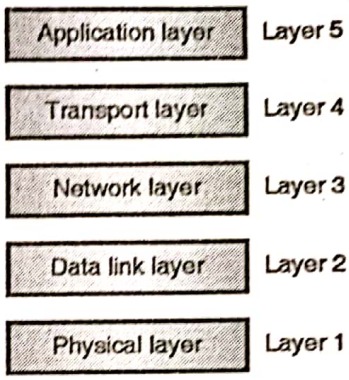
It is a process of inserting a reference marker called as a checkpoint into the data stream travelling between the sending and receiving systems. This allows the checking of status of both the machines at the same point in time. This will avoid any possible confusion and collision situation.

Q. 15 Explain in short TCP/IP model. May 16

Ans. :

TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol. A **protocol suite** is defined as the set of protocols organized in different layers. The TCP/IP protocol suite is used in Internet today.

TCP/IP is a hierarchical protocol suite means that each upper layer protocol receives support and services from either one or more lower level protocols. In the original TCP/IP protocol suite, there were four software layers built upon the hardware. But today's TCP/IP protocol suite uses a five layer model as shown in Fig. 1.8.



(G-2065) **Fig. 1.8 : Layers in TCP/IP protocol suite**

Q. 16 Explain the layer details of TCP/IP models. Dec. 12

Ans. :

Detailed Introduction to Physical Layer

Physical layer is the lowest layer in the TCP/IP protocol suite. The communication at the physical layer level is still **logical** because of the presence of a hidden layer (transmission media) under the physical layer. The **primary responsibility** of the physical layer is to carry the individual bits present in a frame across the link. The transmission media (wired or wireless) is used for connecting two devices to each other. Here it is important to understand that the transmission media does not actually carry the bits. Instead it carries the electrical or optical signals which represents the bits which are to be carried from one device to the other.

That means the bits received in a frame from the data link layer are transformed into an electrical or optical signal and sent over the transmission media. Still we consider **bit** as the data unit for communication between physical layers of two communicating devices. For the transformation of bits to signal, several physical layer protocols are available.

Detailed Introduction to Data Link Layer :

An internetwork consists of many LANs and WANs, connected to each other by routers. While travelling from source to destination a datagram has to travel through many overlapping sets of links. It is the responsibility of router to choose the best possible link for a datagram to travel. When a router does so, it is the responsibility of the data link layer to take the datagram across the link.

The said link can be anything such as a wired LAN, a wireless LAN, or a link layer switch etc. Every type of link will use different types of protocols. The data link layer should be able to handle all the different types of protocols and move the packet through the link. The data link layer receives a datagram from the network layer and encapsulates it into a packet called as **frame.**

There are no specific data link layer protocols defined by the TCP/IP suite. Instead it supports all the standard protocols that can carry the datagram successfully over the link. The services provided by each data link layer protocol are different.

Scanned by CamScanner

Detailed Introduction to Network Layer :

The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication. The several routers present between the source and destination hosts choose the best route for each travelling packet. Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.

The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP. The routing of datagrams from their source to destination is also the responsibility of IP. It achieves this by making each router forward the datagrams to the next router in its path towards the destination. IP is a **connectionless** protocol. It does not provide services like **flow control, error control** or even the **congestion control.** Therefore it is dependent on the transport layer in case if an application needs these services. The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.

These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.

There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks. The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.

The functioning of these protocols is as follows :

Sr. No.	Protocol	Function
1.	ICMP	To help IP report problems when routing a packet
2.	IGMP	Helps IP in multitasking
3.	DHCP	To help IP to get the network layer address for a host.
4.	ARP	Helps IP to find the link layer address of a host or router.

Detailed Introduction to Transport Layer :

The primary responsibility of the transport layer is also to provide an end to end connection. At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.

In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination. For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.

The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol. The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data. Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :

1. Flow control
2. Error control and
3. Congestion control

The other commonly used transport layer protocol is UDP (User Datagram Protocol). This is a connectionless protocol. Therefore it does not need to create any logical connection before transmitting the user datagrams. The UDP treats each datagram as a totally in dependent packet with absolutely no relation with the previous or next datagrams.

UDP is a very simple protocol as compared to TCP. It does not provide flow control, error control or congestion control.

UDP is an attractive protocol for certain application program specially for those who want to send small messages or those who do not afford retransmission of a packet if the packet is corrupted or lost. For new emerging applications in the field of multimedia, a new transport layer protocol has been designed which is called as SCTP (Stream Control Transmission Protocol).

Detailed Introduction to Application Layer :

The logical connection between the application layers of source and destination hosts is **end-to-end** type. The communication between the application layers of source and destination hosts takes place through all the layers.

The application layer communication is between **two processes.** A process is nothing but a program running at the application layer. Thus the primary responsibility of the application layer is the **process to process communication.**

There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc. These protocols and their functions are shown in Table 1.2.

Table 1.2

Sr. No.	Protocol	Function
1.	HTTP	As tool to access World Wide Web i.e. WWW.
2.	SMTP	It is the main protocol used in e-mail service.
3.	FTP	To transfer files from one host to the other.
4.	TELNET	To access a website remotely.
5.	SNMP	To manage the Internet.
6.	DNS	To find the network layer address of a computer.
7.	IGMP	To collect the membership in a group.

Scanned by CamScanner

The application layer performs the following functions :

1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
3. It creates a basis for forwarding and storage of e-mails.

Q. 17 Compare the TCP/IP and OSI reference models. May 12, Dec. 14, May 17, Dec. 17

Ans. :

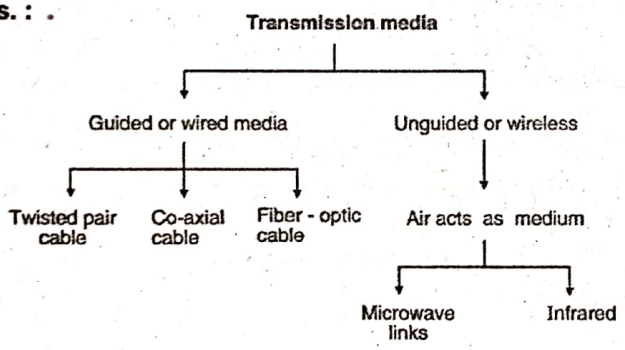
Table 1.3 : Difference between OSI and TCP/IP model

OSI	TCP/IP
Has 7 layers	Has 4 layers
Transport layer guarantees delivery of packets.	Transport layer does not guarantee delivery of packets.
Horizontal approach.	Vertical approach.
Separate session layer.	No session layer, characteristics are provided by transport layer.
Separate presentation layer.	No presentation layer, characteristics are provided by application layer.
Network layer provides both connectionless and connection oriented services.	Network layer provides only connection less services.
It defines the services, interfaces and protocols very clearly and makes a clear distinction between them.	It does not clearly distinguish between service, interfaces and protocols.
The protocols are better hidden and can be easily replaced as the technology changes.	It is not easy to replace the protocols.
OSI is truly a general model.	TCP/IP cannot be used for any other application.
It has a problem of protocol fitting into a model.	The model does not fit any other protocol stack.

Chapter 2 : Physical Layer

Q. 1 What are the different guided and unguided transmission media ? May 17

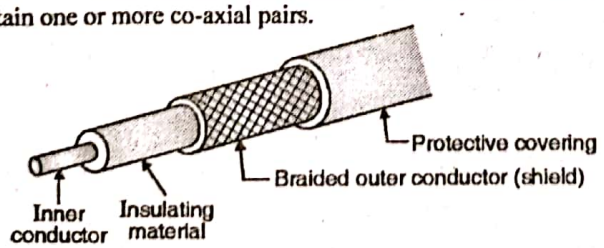
Ans. :



(L-571) **Fig. 2.1 : Classification of transmission media**

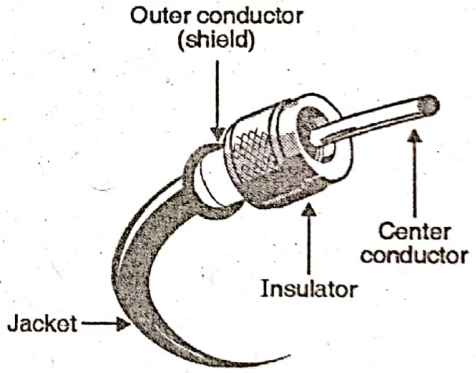
Q. 2 Explain Co-axial Cables. May 07

Ans. : The construction of co-axial cable is as shown in Fig. 2.2. It consists of two concentric conductors namely an inner conductor and a braided outer conductor separated by a dielectric material. The external conductor is in the form of metallic braid and used for the purpose of shielding. The co-axial cable may contain one or more co-axial pairs.



(L-577) **Fig. 2.2 : Construction of a co-axial cable**

The construction of a co-axial cable with other accessories such as connector, jacket etc. is shown in Fig. 2.2(a).



(L-577) **Fig. 2.2(a) : Co-axial cable**

The wire mesh (braided conductor) protects the inner conductor from Electromagnetic Interference (EMI). It is often called a shield. A tough plastic jacket forms the cover of the cable as shown in Fig. 2.2(a) providing insulation and protection. The co-axial cable was initially developed for analog telephone networks. A single co-axial cable would be used to carry more than 10,000 voice channels at a time.

The digital transmission systems using the co-axial cable were developed in 1970s. These systems operated in the range of 8.5 Mb/s to 565 Mb/s.

The most popular application of a co-axial cable is in the cable TV system. The existing co-axial cable system has a range from 54 MHz to 500 MHz. Other important application is cable modem, with the cable modem termination system (CMTS). One more application is Ethernet LAN using the co-axial cable.

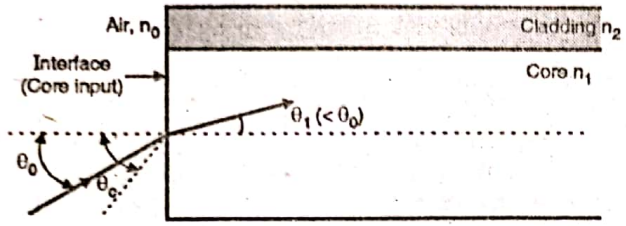
Scanned by CamScanner

The co-axial cable is used for its large bandwidth and high noise immunity.

Q. 3 Explain the modes of propagating light along optical channels. Dec. 14

Ans. :

The number of paths followed by light rays inside the optical cable is called as modes. Fig. 2.3 shows different modes of operation of an optical fiber.



(G-108) **Fig. 2.3 : Propagation modes in optical fibers**

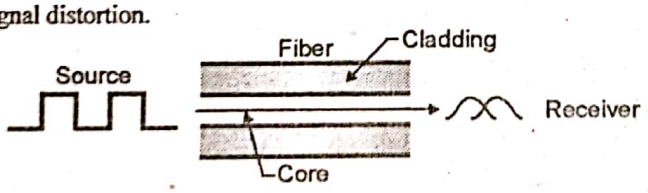
There are two types namely single mode and multimode's fibers. In single mode light follows a single path through the core whereas in multimode, the light takes more than one paths through the core.

Single Mode Fibers :

These are called as single mode fibers because they support on one mode of propagation (TE, TM or TEM).

The optical signal travelling inside this fiber has only one group velocity. Due to single mode travelling, the amount of dispersion is less than that introduced in multimode fibers. These fibers can have either step index or graded index profile. They are high quality fibers used for wideband long haul communication and they are fabricated from doped silica to reduce internal attenuation.

The light travel in a single mode fiber is shown in Fig. 2.3(a). This beam travel's almost horizontally and follows only one path from source to destination, as shown in Fig. 2.3(a). The critical angle of incident highly focused light beam is nearly equal to 90°. In the single mode fibers the delays are negligible and the signal reconstruction at the receiver is easier which results in almost no signal distortion.



(G-109) **Fig. 2.3(a) : Single mode fiber**

Multimode Fibers :

These are called as multimode fibers because they support simultaneous propagation of many modes and the incident light follows different paths from the source to destination. Each mode has its own group velocity and each mode will follow its own path while travelling from the transmitter to receiver. Due to presence of more than one modes, the intermodal dispersion will exist.

Multimode fibers can have the step index or graded index profile and they are fabricated using the multicomponent glasses or doped silica.

Q. 4 List the advantages of fiber optics as a communication medium. Dec. 14, Dec. 16

Ans. :

Some of the advantages of fiber optic communication over the conventional means of communication are as follows :

1. **Small size and light weight :**

   The size (diameter) of the optical fibers is very small (it is comparable to the diameter of human hair). Therefore a large number of optical fibers can fit into a cable of small diameter.

2. **Easy availability and low cost :**

   The material used for the manufacturing of optical fibers is "silica glass". This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.

3. **No electrical or electromagnetic interference :**

   Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.

4. **Large bandwidth :**

   As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fiber is extremely large. This allows transmission of more number of channels. Therefore the information carrying capacity of an optical fiber is much higher than that of a co-axial cable.

Q. 5 Compare the performance characteristics of coaxial, twisted pair and fiber optic transmission media. Dec. 06

Ans. :

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
1.	Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber
2.	Noise immunity is low. Therefore more distortion.	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor.	Highest noise immunity as the light rays are unaffected by the electrical noise.
3.	Affected due to external magnetic field.	Less affected due to external magnetic field.	Not affected by the external magnetic field.

Scanned by CamScanner

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
4.	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
5.	Cheapest	Moderately expensive	Expensive
6.	Can support low data rates.	Moderately high data rates	Very high data rates.
7.	Power loss due to conduction and radiation.	Power loss due to conduction	Power loss due to absorption, scattering, dispersion and bending.
8.	Low bandwidth	Moderately high bandwidth	Very high bandwidth
9.	Node capacity per segment is 2	Node capacity per segment is 30 to 100	Node capacity per segment is 2.
10.	Attenuation is very high	Attenuation is low	Attenuation is very low.
11.	Installation is easy	Installation is fairly easy	Installation is difficult.
12.	Electromagnetic interference (EMI) can take place	EMI is reduced due to shielding	EMI is not present.

Q. 6 Write short notes on : Bluetooth.

Dec. 05, Dec. 06, May 07, May 08, Dec. 08, Dec. 10, May 11, Dec. 11, Dec. 12, May 13, Dec. 13, May 17

Ans. :

Bluetooth is the name given to a new technology using short-range radio links, which could replace the cable(s) connecting portable and/or fixed electronic devices.

Bluetooth replaces cables that connect one device to another with one universal radio link. Its key features are robustness, low complexity, low power and low cost. Designed to operate in noisy frequency environments, the Bluetooth radio uses a fast acknowledgement and frequency-hopping scheme to make the link more reliable.

Bluetooth radio modules operate in the unlicensed ISM band at 2.4 GHz, and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. Compared with other systems in the same frequency band, the Bluetooth radio hops faster and uses shorter wavelengths.

Thus Bluetooth is a wireless LAN technology which can connect devices such as telephones, computers, printers, cameras, etc. without using wires. A Bluetooth LAN is an Ad hoc network i.e. it does not use a base station. It is possible to connect the Bluetooth LAN to the Internet. This technology is implemented using the IEEE 802.15 standard.

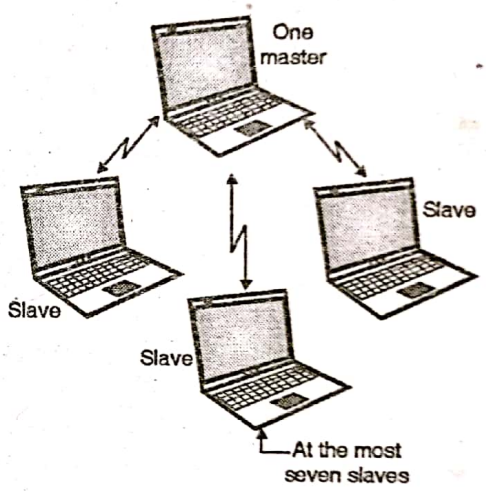
Architecture :

1. Piconets and 2. Scatternets.

Piconets :

The first type of Bluetooth network is called as a **piconet** or a **small net**. It can have at the most eight stations. One of them is called as a **master** and all others are called as **slaves.** All the slave stations are synchronised in all aspects with the master. A piconet can have only one master station. Fig. 2.4 shows a piconet. A master can also be called as a primary station and slaves are secondary station.

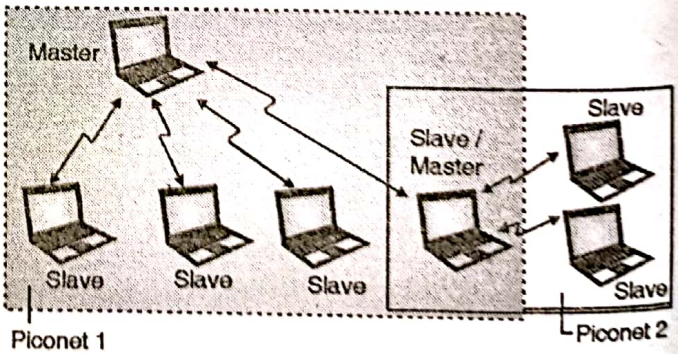
The communication between a master and slaves can be one-to-one or one-to-many. Note that the communication takes place between the master and slaves but no direct communication takes place between the slaves.



(G-388)**Fig. 2.4 : A piconet**

Scatternet :

A scatternet is obtained by combining piconets as shown in Fig. 2.4(a).



(G-389) **Fig. 2.4(a) : Scatternet**

Fig. 2.4(a) shows a scatternet consisting of two piconets. A slave in the first piconet can act as a master in the second piconet. It will receive the messages from the master in the first piconet by acting as a slave and then delivers the message to the slaves in the second piconet as shown in Fig. 2.4(a). So the same device acts as a slave in the first piconet and as master in the second piconet.

Scanned by CamScanner

Q. 7 Compare and contrast a circuit switching and a packet switching network. May 17

Ans. :

Parameter	Circuit switching	Packet switching
Application	Telephone network for bi-directional, real time transfer of voice signals.	Internet for datagram and reliable stream service between computers.
End terminal	Telephone, modem.	Computer
Information type	Analog voice or PCM digital voice	Binary information
Transmission system	Analog and digital data over different transmission media	Digital data over different transmission media.
Addressing scheme	Hierarchical numbering plan	Hierarchical address space
Routing scheme	Route selected during call setup.	Each packet is routed independently.
Multiplexing scheme	Circuit multiplexing.	Packet multiplexing shared media access networks.

Chapter 3 : Data Link Layer

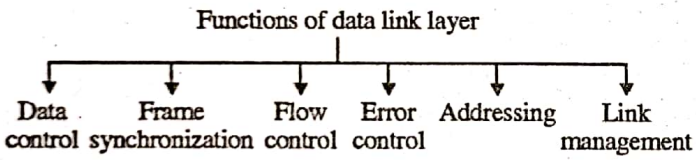
Q. 1 Enumerate the main responsibilities of the data link layer.

Dec. 06, Dec. 07, May 10, May 11, May 16, May 17

Ans. :

The data link layer is supposed to carry out many specified functions.

For effective data communication between two directly (physically) connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows :



(L-664)**Fig. 3.1 : Functions of data link layer**

1. **Services provided to the network layer :**

   The data link layer provides a well defined service interface to the network layer. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via the DLL.

2. **Frame synchronisation :**

   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**

   The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control :**

   The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. **Addressing :**

   When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames. This is known as addressing.

6. **Control and data on same link :**

   The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to separate out the control information from the data being transmitted.

7. **Link management :**

   The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data. It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

Q. 2 Why there is a need for framing ?

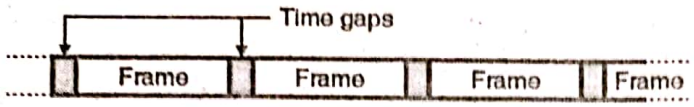
Dec. 09, Dec. 11, Dec. 14

Ans. :

The bits to be transmitted is first broken into discrete frames at the data link layer. In order to guarantee that the bit stream is error free, the checksum of each frame is computed. When a frame is received, the data link there, recomputes the checksum. If it is different from the checksum present in the frame, then the data link layer knows that an error has occurred.

It then discards the bad frame and sends back a request for retransmission. Breaking the bit stream into frames is called as framing. One way of doing it is by inserting time gaps between frames as shown in Fig. 3.2.

Scanned by CamScanner



(G-178) **Fig. 3.2 : Framing**

But practically this framing technique does not work satisfactorily, because networks generally do not make any guarantees about the timing.

Q. 3 Explain the different framing methods.

Dec. 10, May 11, May 13, Dec. 14, May 15, May 16, Dec. 17

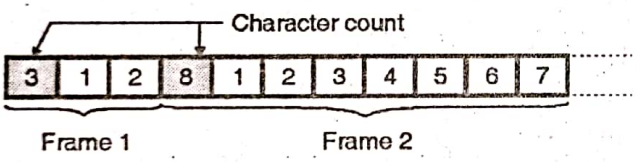
Ans. :

1. Character count method.
2. Starting and ending characters, with character stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

Character Count :

In this method, a field in the header is used to specify the number of characters in the frame. This number helps the receiver to know the exact number of characters present in the frame following this count.

The character count method is illustrated in Fig. 3.3.



(L-668)**Fig. 3.3 : Character count method**

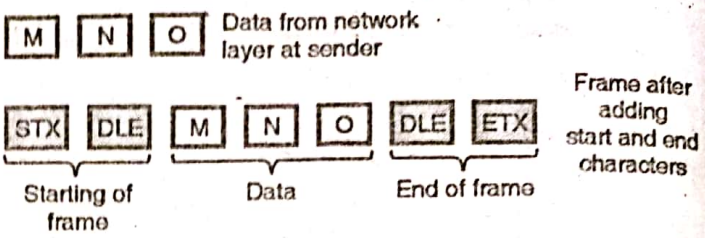
The two frames shown in Fig. 3.3 contain 3 and 8 characters respectively and numbers 3 and 8 are inserted in the headers of the corresponding frames. The disadvantage of this method is that, an error can change the character count itself.

If the wrong character count number is received due to error then the receiver will get out of synchronization and will not be able to locate the start of next frame. The character count method is rarely used in practice.

Starting and Ending Character with Character Stuffing :

The problem of character count method is solved here by using a starting character before the starting of each frame and an ending character at the end of each frame. Each frame is preceded by the transmission of ASCII character sequence DLE STX. (DLE stands for data link escape and STX is start of TeXt).

After each frame the ASCII character sequence DLE ETX is transmitted. Here DLE stands for Data Link Escape and ETX stands for End of TeXt. So if the receiver loses the synchronization, it just has to search for the DLE STX or DLE ETX characters to return back on track. This is shown in Fig. 3.3(a).



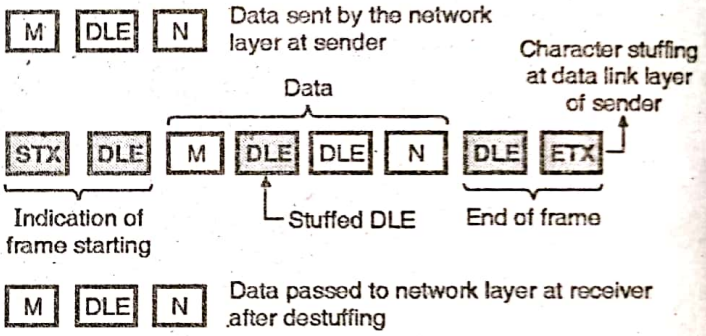
(L-669)**Fig. 3.3(a)**

Character Stuffing :

The problem with this system is that the characters DLE STX or DLE ETX can be a part of data as well.

If so, they will be misinterpreted by the receiver as start or end of frame. This problem is solved by using a technique called **character stuffing** which is as follows.

The data link layer at the sending end inserts an ASCII DLE character just before each accidental DLE character in the data being transmitted. The data link layer at the receiving end will remove these DLE characters before transferring the data to the network layer.



(G-181) **Fig. 3.3(b) : Character stuffing**

Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once. This is called character stuffing and it is shown in Fig. 3.3(b). Note that at the receiving end the destuffing is essential. Destuffing process is exactly opposite to the character stuffing process.

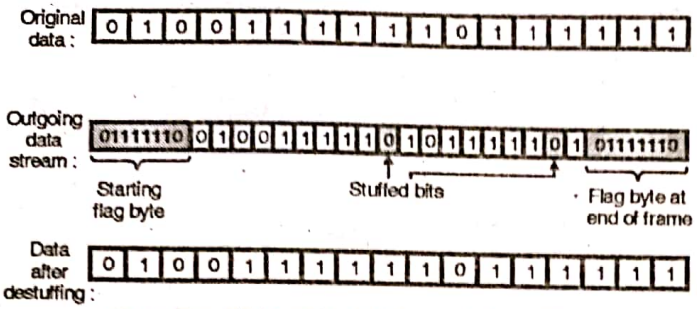
Starting and Ending Flags, with Bit Stuffing :

In this framing techniques at the beginning and end of each frame, a specific bit pattern 0111 1110 called **flag byte** is transmitted by the sending station. Since there are six consecutive 1s in the flag byte a technique called **bit stuffing** which is similar to character stuffing is used. It is as explained below.

Bit stuffing :

Whenever the sender data link layer detects the presence of five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing bit stream. Thus the six consecutive 1s will never appear in the data stream. Hence there is no chance of misinterpretation. This is called bit stuffing and it is illustrated in Fig. 3.3(c).

Scanned by CamScanner

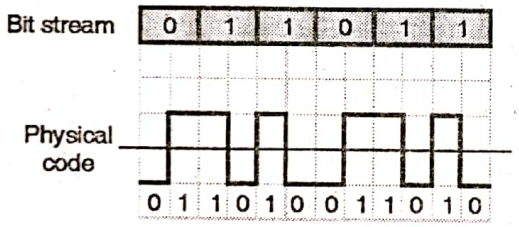


(G-183) **Fig. 3.3(c) : Bit stuffing and destuffing**

When a receiver detects presence of five consecutive ones in the received bit stream, it automatically deletes the 0 bit following the five ones. This is called de-stuffing. It is shown in Fig. 3.3(c). Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

Physical Layer Coding Violations :

This method of framing is applicable only to those networks in which the encoding on the physical medium contains some redundancy. Some LANs encode each bit of data using two physical bits for example the use of the Manchester coding refer Fig. 3.3(d). The physical Manchester code makes a transition at the middle of the bit interval.as shown. Therefore a 1 bit is encoded into a 10 pair and a 0 bit is encoded into a 01 pair as shown in Fig. 3.3(d). This helps in recognizing the boundaries of bits in a precise manner. This use of invalid physical code is a part of 802 LAN standards.



(G-184)**Fig. 3.3(d)**

Q. 4 Explain with the suitable example CRC algorithm for computing checksum.

May 09, Dec. 12, May 13

Ans. :

This is a type of polynomial code in which a bit string is represented in the form of polynomials with coefficients of 0 and 1 only. Polynomial arithmetic uses a modulo-2 arithmetic i.e. addition and subtraction are identical to EXOR. For CRC code the sender and receiver should agree upon a generator polynomial G(x). A codeword can be generated for a given dataword (message) polynomial M(x) with the help of long division. This technique is more powerful than the parity check and checksum error detection.

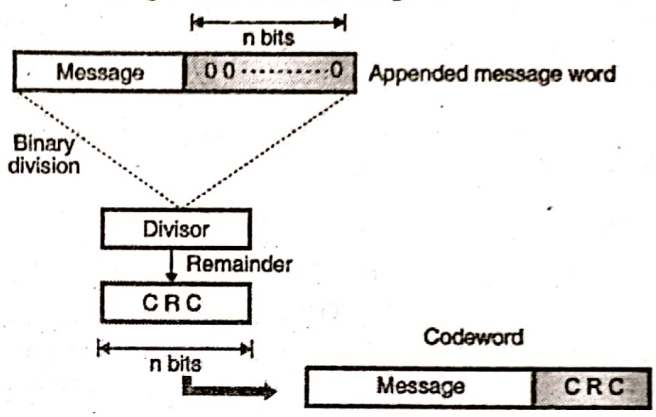
CRC works on the principle of binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of the message. We will call this word as appended message word. The appended word thus obtained becomes exactly divisible by the generator word corresponding to G (x).

The sender appends the CRC to the message word to form a codeword. At the receiver, this codeword is divided by the same generator word which corresponds to G (x).

There is no error if the remainder of this division is zero. But a non-zero remainder indicates presence of errors in the received codeword. Such an erroneous codeword is then rejected.

CRC generator :

The CRC generator is shown in Fig. 3.4.



(L-819) **Fig. 3.4 : CRC generator**

The stepwise procedure in CRC generation is as follows :

Step 1 : Append a train of n 0s to the message word where n is 1 less than the number of bits in the predecided divisor (i.e. generator word). If the divisor is 5-bit long then we have to append 4-zeros to the message.

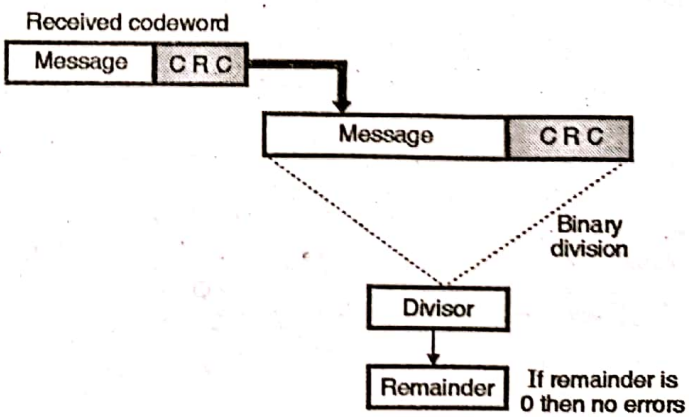
Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.

Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 3.4.

CRC checker :

Fig. 3.4(a) shows the CRC checker.



(L-820) **Fig. 3.4(a) : CRC checker**

Scanned by CamScanner

The codeword received at the receiver consists of message and CRC. (Fig. 3.4(a)) The receiver treats it as one unit and divides it by the same (n + 1) bit divisor (generator word) which was used at the transmitter. The remainder of this division is then checked. If the remainder is zero, then the received codeword is error free and hence should be accepted. But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

Q. 5 Explain the error detection and error correction algorithms. Dec. 12

Ans. :

Here we see two completely different approaches for the error control. They are :

1. Forward error correction (FEC)
2. Automatic request for retransmission (ARQ).

The ARQ technique : In the ARQ system, the receiver can request for the retransmission of the complete or a part of message if it finds some error in the received message. This needs an additional channel called feedback channel to send the receiver's request for retransmission.

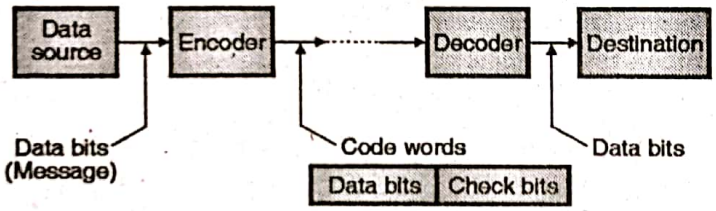
The FEC technique : In the FEC technique there is no such feedback path and request for retransmission. So error correction has to take place at the receiver.

Error correction techniques :

In the error correction techniques, codes are generated at transmitter by adding a group of parity bits or check bits as shown in Fig. 3.5.

The source generates the data (message) in the form of binary symbols. The encoder accepts these bits and adds the check (parity) bits to them to produce the code words.

These code words are transmitted towards the receiver. The check bits are used by the decoder to detect and correct the errors.

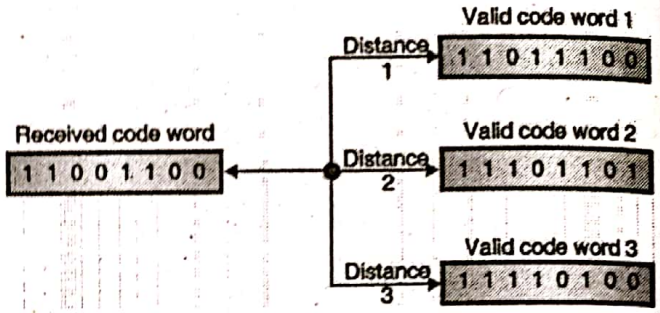


(L-306) **Fig. 3.5 : Error correction technique**

The encoder of Fig. 3.5, adds the check bits to the data bits, **according to a prescribed rule.** This rule will be dependent on the type of code being used. The decoder separates out the data and check bits. It uses the parity bits to detect and correct errors if they are present in the received code words. The data bits are then passed on to the destination.

FEC (Forward Error Correction) :

In FEC the receiver searches for the most likely correct code word. When an error is detected, the distance between the received invalid code word and all the possible valid code words is obtained. The nearest valid code word (the one having minimum distance) is the most likely the correct version of the received code word as shown in Fig. 3.5(a).



(L-307) **Fig. 3.5(a) : Concept of FEC**

In Fig. 3.5(a), the valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

Error correction techniques :

Some of the FEC techniques are as follows :

1. Linear block codes.
2. Convolutional coding.
3. Hamming codes.
4. Cyclic codes.

Q. 6 If the frame is 1101011011 and generator is $x^4 + x + 1$ what would be the transmitted frame. May 05, Dec. 09, May 11

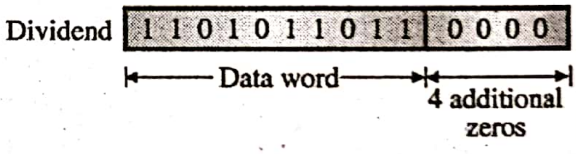
Ans. :

Given : Data word : 1 1 0 1 0 1 1 0 1 1

Generator : $x^4 + x + 1 = x^4 + 0x^3 + 0x^2 + x + 1 = 10011 = n$

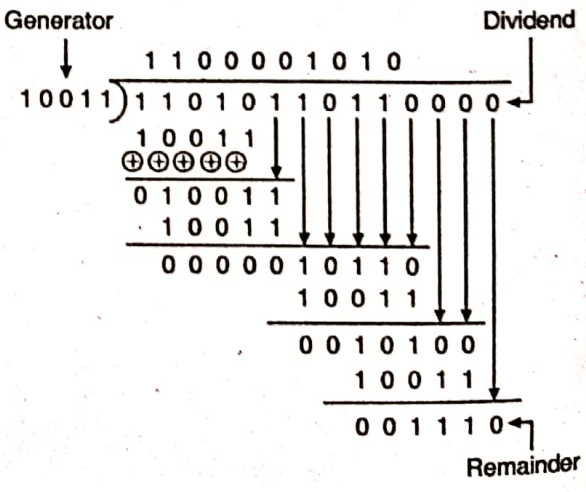
Step 1 : Add four zeros at the end of the data word :

Add four zeros (n – 1) at the end of data word to get the dividend as follows :



(G-216(c))

Step 2 : Carryout the long division :



(G-216(d))

Scanned by CamScanner

Step 3 : Write the transmitted frame :

The transmitted frame is obtained by writing the data word followed by the remainder.

$\therefore$ 1 1 0 1 0 1 1 0 1 1 0 0 0 0 ← Dividend

1 1 1 0 ← Remainder

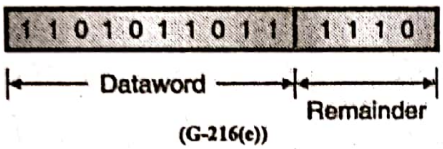
\+

1 1 0 1 0 1 1 0 1 1 1 1 1 0

Transmitted frame

(G-1967)

$\therefore$ The transmitted codeword is as follows :



(G-216(e))

Q. 7 Consider an error detecting CRC with the generator 10101. Assume the CRC bits follows the data bits in any transmission :

1. **Compute the transmitted bit sequence for the data bit sequence 01101101.**
2. **The string of bits 110011001100 is received. Is it acceptable, and if so what is the data bit sequence.** Dec. 03

Ans. :

Part I : Transmitted bit sequence :

Given : Data bit sequence : 0 1 1 0 1 1 0 1

Generator : 1 0 1 0 1

Step 1 : Append 4 zeros to the data bit sequence :

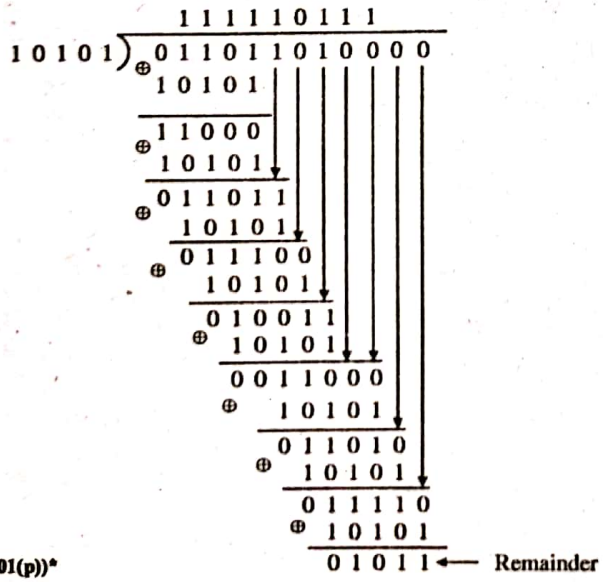
Dividend = Data word + 4 zeros

= 0 1 1 0 1 1 0 1 | 0 0 0 0

Data bit sequence — 4 Zeros

(G-801(o))

Step 2 : Carry out division :



(G-801(p))*

Step 3 : Codeword :

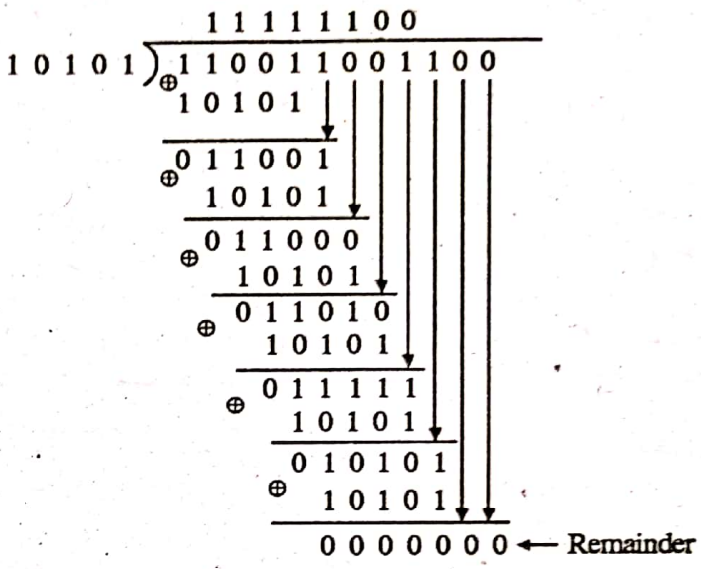
Codeword = Dividend + Remainder

= 0 1 1 0 1 1 0 1 | 1 0 1 1

Part II :

Received word : 1 1 0 0 1 1 0 0 1 1 0 0

Carry out the division as follows :



(G-801(q))

Since the remainder is 0, the received codeword is acceptable and does not contain errors. So it is acceptable.

Received codeword = 1 1 0 0 1 1 0 0 | 1 1 0 0

(G-801(r))

Q. 8 Consider an error detecting CRC with the generator 10101.

1. **Compute the transmitted bit sequence for the data bit sequence 1101101.**
2. **The string of bits 110011001100 is received. Is acceptable, and if so what is the data bit sequence.** Dec. 05

Ans. :

Part I : Transmitted bit sequence :

Given : Data bit sequence : 1 1 0 1 1 0 1

Generator : 1 0 1 0 1

Step 1 : Obtain the dividend :

Dividend = Data word followed by 4 zeros.

= 1 1 0 1 1 0 1 0 0 0 0

Scanned by CamScanner

Step 2 : Carry out division :

```
                1 1 1 0 1 1 1
          ---------------------
1 0 1 0 1 ) 1 1 0 1 1 0 1 0 0 0 0
            ⊕ 1 0 1 0 1
            -------------
              0 1 1 1 0 0
            ⊕   1 0 1 0 1
              -------------
              0 1 0 0 1 1
            ⊕   1 0 1 0 1
              -------------
              0 0 1 1 0 0 0
            ⊕     1 0 1 0 1
              -------------
              0 1 1 0 1 0
            ⊕   1 0 1 0 1
              -------------
              0 1 1 1 1 0
            ⊕   1 0 1 0 1
              -------------
                1 0 1 1   ← Remainder
```

(G-801(t))

Step 3 : Transmitted bit sequence :

The transmitted bit sequence is obtained by adding remainder to the dividend.

∴ Transmitted code word = 1 1 0 1 1 0 1 | 1 0 1 1

Data bits | Remainder

(G-801(u))

Part II :

The received bit sequence is 1100 1100 1100. Divide it by the same generator used in part I.

```
                1 1 1 1 1 1 0 0
          ---------------------
1 0 1 0 1 ) 1 1 0 0 1 1 0 0 1 1 0 0
            ⊕ 1 0 1 0 1
            -------------
              0 1 1 0 0 1
            ⊕   1 0 1 0 1
              -------------
              0 1 1 0 0 0
            ⊕     1 0 1 0 1
              -------------
              0 1 1 0 1 0
            ⊕   1 0 1 0 1
              -------------
              0 1 1 1 1 1
            ⊕   1 0 1 0 1
              -------------
              0 1 0 1 0 1
            ⊕   1 0 1 0 1
              -------------
              0 0 0 0 0 0 0  ← Remainder
```

(G-801(v))

Since the remainder is zero, there are no errors in the received bit sequence. Hence it is acceptable. The received sequence is,

1 1 0 0 1 1 0 0 | 1 1 0 0

← Bit sequence → | ← Remainder →

(G-801(w))

∴ Received bit sequence = 1 1 0 0 1 1 0 0 ...Ans.

Q. 9 An 8-bit byte with binary value 10101111 is to be encoded using an even-parity Hamming code. What is the binary value after encoding ?

Dec. 10, Dec. 11, May 12

Ans. :

Data number : 10101111

Step 1 :

Number of message bits are 8. So we need to add 4 parity bits in the codeword.

The parity bits will be at the positions 1, 2, 4 and 8 as shown in Fig. 3.6.

D_{12}	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	0	P	1	1	1	P	1	P	P

Fig. 3.6

Step 2 : Select P_1 for P_1 D_3 D_5 D_7 D_9 D_{11} :

Parity needs to be even parity.

D_{11}	D_9	D_7	D_5	D_3	
0	0	1	1	1	P_1

Fig. 3.6(a)

For even parity P_1 should be 1.

∴ P_1= 1

Step 3 : Select P_2 for P_2 D_3 D_6 D_7 D_{10} D_{11} :

D_{11}	D_{10}	D_7	D_6	D_3	
0	1	1	1	1	P_2

Fig. 3.6(b)

∴ P_2= 0

Step 4 : Select P_4 for P_4 D_5 D_6 D_7 D_{12} :

D_{12}	D_7	D_6	D_5	
1	1	1	1	P_4

Fig. 3.6(c)

∴ P_4= 0

Step 5 : Select P_8 for P_8 D_9 D_{10} D_{11} D_{12} :

D_{12}	D_{11}	D_{10}	D_9	
1	0	1	0	P_8

Fig. 3.6(d)

∴ P_8= 0

So codeword is as follows,

				P_8				P_4		P_2	P_1
Codeword :	1	0	1	0	0	1	1	1	0	1	0	1

Fig. 3.6(e)

Q. 10 Compute the Hamming code for the data - 1001101.

Dec. 13

Scanned by CamScanner

Ans. :

Step 1 : Codeword format :

11	10	9	8	7	6	5	4	3	2	1
1	0	0	P_8	1	1	0	P_4	1	P_2	P_1

(G-2278) **Fig. 3.7 : Codeword format**

Step 2 : Find : P_1, P_2, P_4, P_8 :

Assume even parity.

1. P_1 :

Consider bits 1,3,5,7,9,11 They are,
10101 P_1 ∴ For even parity $P_1 = 1$

2. P_2 :

Consider bits 2,3,6,7,10,11 They are,
10111 P_1 ∴ For even parity $P_2 = 0$

3. P_4 :

Consider bits 4,5,6,7 They are,
110 P_4 ∴ For even parity $P_4 = 0$

4. P_8 :

Consider bits 8,9,10,11 They are,
1 0 0 P_8 ∴ For even parity $P_8 = 1$

Step 3 : Write the codeword :

Code word =	1	0	0	1	1	1	0	0	1	0	1

Q. 11 Explain stop and wait sliding window protocol.

Dec. 03, May 07, Dec. 08, Dec. 09

Ans. :

In the simplex stop and wait protocol it is assumed that a finite processing time is essential.

However like the first protocol, the communication channel is assumed to be noise free and the communication is simplex i.e. only in one direction at a given time.

This protocol deals with an important problem i.e. how to prevent the sender from flooding the receiver due to the data rates faster than processing speed of the receiver. In this protocol, a small dummy frame is sent back from the receiver to the transmitter to indicate that it can send the next frame. The small dummy frame is called as acknowledgement. The transmitter sends one frame and then waits for the dummy frame called acknowledgement. Once the acknowledgement is received, it sends the next frame and waits for the acknowledgement. Hence this protocol is known as **stop and wait** protocol The best thing about this protocol is that the incoming frame is always an acknowledgement. It need not be even checked.

Q. 12 Describe in brief piggybacking. Dec. 07

Ans. :

In all the practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission.

One way of achieving full duplex transmission is to have two separate channels one for forward data transmission and the other for reverse data transfer (for acknowledgements). But this will waste the bandwidth of the reverse channel almost entirely.

A better solution would be to use each channel (forward and reverse) to transmit frames both ways, with both channels having the same capacity. Let A and B be the users. Then the data frames from A to B are intermixed with the acknowledgements from A to B. By checking the kind field in the header of the received frame the received frame can be identified as either data frame or acknowledgement.

One more improvement can be made. When a data frame arrives, the receiver waits, does not send the control frame (acknowledgement) back immediately. The receiver waits until its network layer passes in the next data packet.

The acknowledgement is then attached to this outgoing data frame. Thus the acknowledgement travels alongwith next data frame. This technique in which the outgoing acknowledgement is delayed temporarily is called as **piggybacking**.

Advantage of piggybacking :

The major advantage of piggybacking is better use of available channel bandwidth. This happens because an acknowledgement frame need not be sent separately.

Disadvantages :

1. The disadvantage of piggybacking is the additional complexity.
2. If the data link layer waits too long before transmitting acknowledgement, then retransmission of frame would take place.

Q. 13 Explain stop and wait and sliding window protocol.

Dec. 03, May 05, May 07, Dec. 08, Dec. 09

Ans. :

The next three protocols are more robust and bi-directional protocols.

All these protocols are special type of protocol called **Sliding Window Protocols.**

They show a different performance in terms of their efficiency, complexity and buffer requirements.

Sequence number :

One of the important features of all the sliding window protocols is that each outbound frame contains a sequence number, ranging from 0 to some maximum value. The maximum value is generally equal to $(2^n - 1)$. The value of n can be arbitrary.

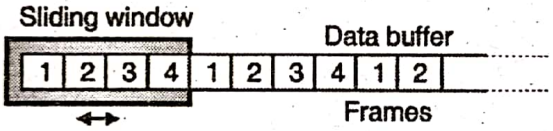
Scanned by CamScanner

Sliding windows :

Sliding windows are basically the imaginary boxes at the transmitter and receiver. This window holds the frames at the transmitting as well as receiving ends and provides the upper limit on the number of frames that can be transmitted before acknowledgement is obtained. So in short we can say that, at any instant of time, the sender maintains a set of sequence numbers corresponding to the frames it is permitted to send. These frames which are being permitted to sent are said to be residing inside the **sending window.** The receiver also maintains a **receiver window.** It corresponds to the set of frames that the receiver is permitted to accept. The sender and receiver windows can be of different sizes.

The positive or negative acknowledgement (ACK or NAK) should be used after every frame. That means the sender sends frame, waits for the acknowledgement and sends the next frame or retransmits the original one, only after receiving either positive or negative acknowledgement from the receiver. In order to improve the efficiency, the sender sends multiple frames at time, the receiver checks the CRC of all the frames one by one and sends one acknowledgement for all the frames. This is the principle of operation of sliding window technique.

In this technique, an imaginary window consisting of "n" number of data frames is defined. This means that upto n number of frames can be sent before receiving an acknowledgement. This is known as sliding window because this window can slide over the data buffer to be sent as shown in Fig. 3.8(a).



(G-222)**Fig. 3.8(a) : Sliding window**

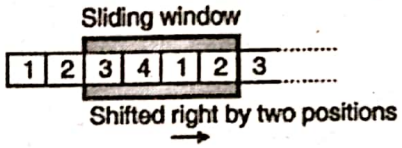
In Fig. 3.8(a) we have shown a sliding window of size n = 4. That means the sender can send four frames, at a time and then wait for the acknowledgement for the receiver. So there will be one acknowledgement corresponding to four sent frames.

Note the numbering of frames in Fig. 3.8(a). As the window size is 4, the frame numbering is 1, 2, 3, 4 then again 1, 2, 3, ... the maximum frame number is restricted to n.

Sender and receiver sliding windows :

The sender as well as the receiver maintain their own sliding windows. The sender sends the number of frames allowed by the size of its own sliding window and then waits for an acknowledgement from the receiver. The receiver sends an acknowledgement which includes the number of the next frame that the sender should send. For example if the sender has sent frames 1 and 2 to the receiver and if receiver receives them correctly, then the acknowledgement sent by the receiver will include number-3 indicating the sender to send frame number-3.

Now if the sender transmits the first 4 frames as per the size of its window and receives an acknowledgement for the first two frames, then the sender will slide its window two frames to the right as shown in Fig. 3.8(b) and sends 5th and 6th frames (i.e. frames 1 and 2 of the next lot).



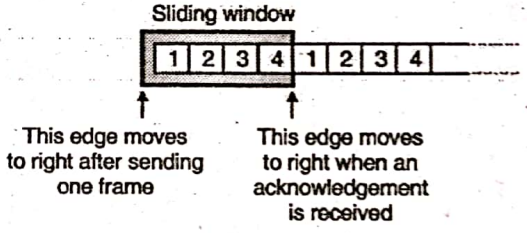
(G-223)**Fig. 3.8(b) : Illustration of sliding window mechanism**

The receiver now has four frames again, so it checks frames 3, 4, 1, 2 by checking their CRC. If it finds frame 3 faulty then it will send an acknowledgement which includes number 3. The sender will send 4-frames staring from frame-3 onwards. The sliding window mechanism thus uses two buffers and one window so as to exercise the flow control. The application program on the sender side will create the data to be transmitted and loads into the sender's buffer.

Then the sender's sliding window is imposed on this buffer. These frames are then sent till all the frames have been sent. The receiver receives these data frames and carriers out checks such as CRC, missing or duplicate frames etc. and stores the correct frames in the receiver buffer. The application program at the receiver then the takes this data.

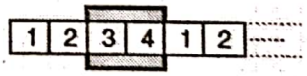
Movement of sender's window :

Fig. 3.8(c) shows the sender's window.



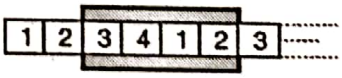
(G-224)**Fig. 3.8(c) : Sender sliding window**

If the senders window size is 4 and frames 1 and 2 are sent but acknowledgement has not been received so far, then as shown in Fig. 3.8(d), the sender's windows will only contain two frames i.e. 3 and 4.



(G-225)**Fig. 3.8(d) : Sender's window after sending first two frames but no acknowledgement**

Now if the sender receives acknowledgement bearing number 3 then it understands that the receiver has correctly received frames 1 and 2. The senders window now expands and includes the next two frames as shown in Fig. 3.8(e).



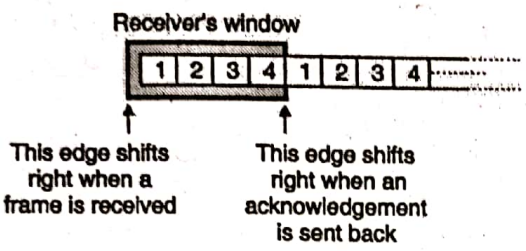
(G-226)**Fig. 3.8(e) : Sender's window after receiving acknowledgement bearing number-3**

In this way the left edge of senders window will shift right when the data frames are sent and the right edge of the senders window will shift right when the acknowledgement is received.

Scanned by CamScanner

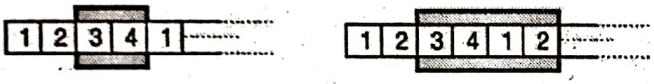
Movement of receiver's windows :

Fig. 3.8(f) shows the receiver's window. Its left edge shifts right on receiving each data frame, where as its right edge shifts right when an acknowledgement is sent.



(G-227)**Fig. 3.8(f) : Receiver's sliding window**

If we take the same explanation that we have seen for the sender's window then the position of receivers windows are as shown in Fig. 3.8(g) and (h).



(g) Two frames (1 and 2) received but no acknowledgement sent **(h) After sending the acknowledgement**

(G-228)**Fig. 3.8 : Movement of receiver window**

Q. 14 Explain a one - bit sliding window protocol in detail. May 04, May 05, Dec. 05, May 10

Ans. :

This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1. It uses the stop-and-wait technique. The sender sends one frame and waits to get its acknowledgement. The sender transmits its next frame only after receiving the acknowledgement for the earlier frame. So one bit sliding window protocol is also called as **stop and wait protocol.** The sequence of events taking place when a frame is transmitted and received is as follows :

1. The data link layer of the sending machine fetches the first packet from its network layer.
2. It builds the frame for it and sends it to receiver.
3. The receiver data link layer checks the received frame for duplication.
4. If ok, it passes the frame to its network layer.

(G-234)

The operation of protocol :

The operation of this protocol is based on the ARQ (automatic repeat request) principle. So the sliding window protocols are also called as ARQ protocols. In this method the transmitter transmits one frame of data and waits for an acknowledgement from the receiver. If it receives a positive acknowledgement (ACK) it transmits the next frame. If it receives a negative acknowledgement (NAK) it retransmits the same frame.

Features added for retransmission :

For retransmission, four features are added to the basic flow control mechanism.

1. The transmitter stores the copy of last frame transmitted until an acknowledgement for that frame is received from the destination.
2. For distinctly identifying different types of frames both data and ACK frames are numbered alternately 0 and 1. The first data frame sent is numbered as 0. This frame is acknowledged by an ACK 1 frame. After receiving ACK1 the sender sends next data frame having a number 1.
3. If an error occurs while transmission, the receiver sends a NAK frame back to the transmitter for retransmission of the corrupted frame. NAK frames which are not numbered tell the transmitter to retransmit the last frame transmitted.
4. The transmitter has a timer to take care of the frame ACK which are lost. After a specified time if the transmitter does not receive a ACK or NAK frame it retransmits the last frame.

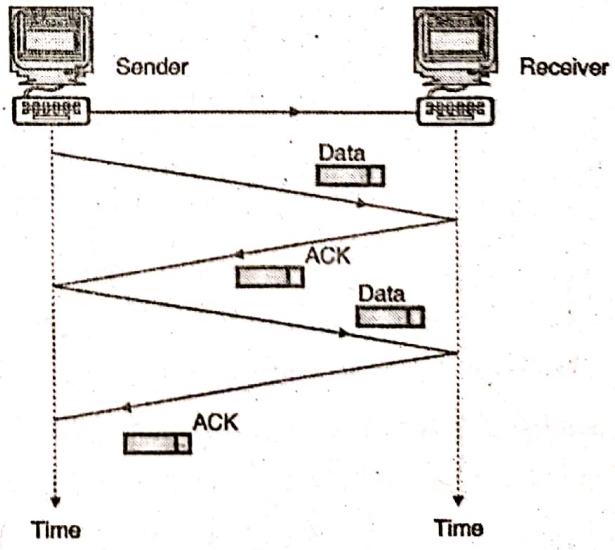
When is the retransmission necessary ?

The retransmission of frame is essential under the following events :

1. If the received frame is damaged.
2. If the transmitted frame is lost.
3. If the acknowledgement from the receiver is lost.

Operation under normal condition :

Fig. 3.9 illustrates the protocol operation when everything is normal. No frame is lost so retransmission is not necessary.

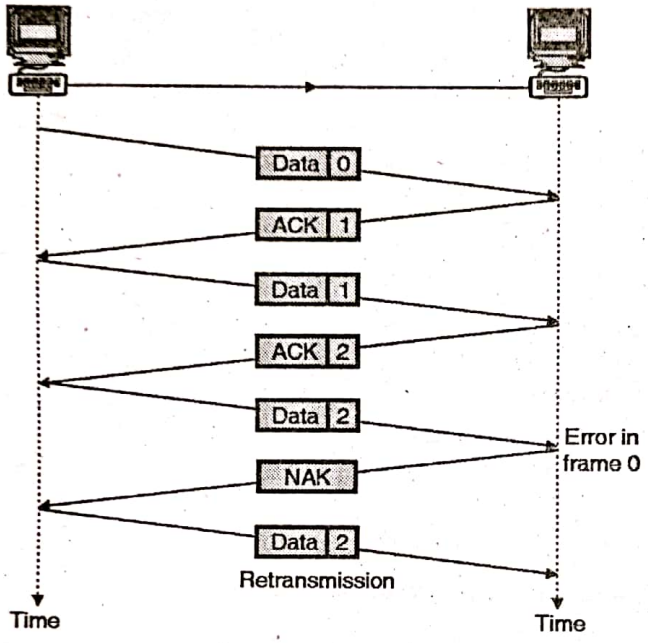


(G-235)**Fig. 3.9 : Stop and wait under normal condition**

Scanned by CamScanner

Stop and wait ARQ for damaged frame :

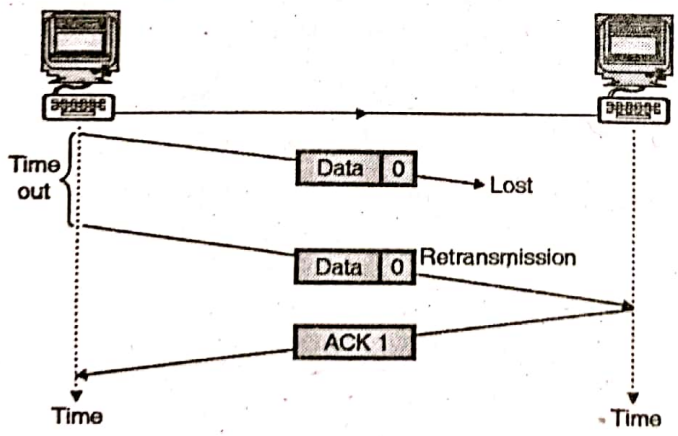
As seen in Fig. 3.9(a) the transmitter transmits data frame numbered 0. The receiver returns an ACK 1 indicating that the data frame numbered 0 is received without any error. The next data frame i.e. data 1 is sent. The corresponding acknowledgement ACK2 is received. The process goes on in this way, but if an error occurs the receiver sends a NAK requesting retransmission of the corrupted data frame (data 2). So the transmitter retransmits the data frame 2.



(G-236)**Fig. 3.9(a) : Stop and wait ARQ damaged frame**

Stop and wait ARQ for lost data frame :

Fig. 3.9(b) shows that if a data frame is lost and if the transmitter does not receive any type of acknowledgement from the receiver with a specified time it retransmits the same frame again.

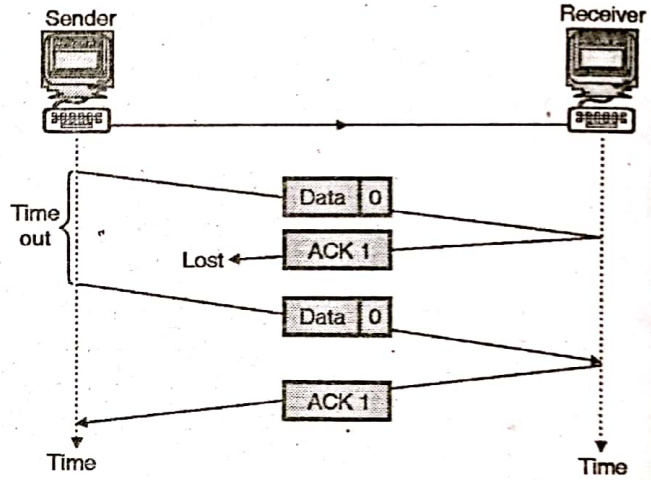


(G-237)**Fig. 3.9(b) : Stop and wait ARQ, lost data frame**

Stop and wait ARQ for lost acknowledgement :

Fig. 3.9(c) shows that if the acknowledgement sent by the receiver is lost, the transmitter retransmits the same data frame after its timer goes off. Stop and wait ARQ protocol becomes inefficient when the propagation delay is much greater than the time to transmit a frame. e.g. assume that we are transmitting frames that are 800 bits long over a channel that has a speed of 1 Mbps and assume that the time taken for transmission of the frame and its acknowledgement is 30 mS. The number of bits that can be transmitted over this channel in 30 mS is equal to $30 \times 10^{-3} \times 1 \times 10^{6} = 30{,}000$ bits. But in the stop-and-wait ARQ only 800 bits can be transmitted in this time period. This inefficiency is due to the fact that in stop and wait ARQ the transmitter waits, for an acknowledgement from the receiver before sending the next frame.

The product of the bit rate and the delay that elapses before an action can take place is called the Delay-bandwidth product. The Delay-bandwidth product helps in measuring the lost opportunity in terms of transmitted bits.



(G-238)**Fig. 3.9(c) : Stop and wait ARQ, lost ACK frame**

Note : Stop-and Wait ARQ was used in IBM's Binary Synchronous Communications (Bisync) Protocol. It is also used in Xmodem, a popular file transfer protocol for modem.

Disadvantages of stop and wait protocol :

1. Problem with Stop-and-Wait protocol is that it is very inefficient. At any one moment, only one frame is in transition.
2. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

Q. 15 Which protocol Go-Back-N or selective-repeat makes more efficient use of network bandwidth ? Why ?

Dec. 03, Dec. 04, Dec. 10, May 11, Dec. 11, Dec. 14, May 15, Dec. 17

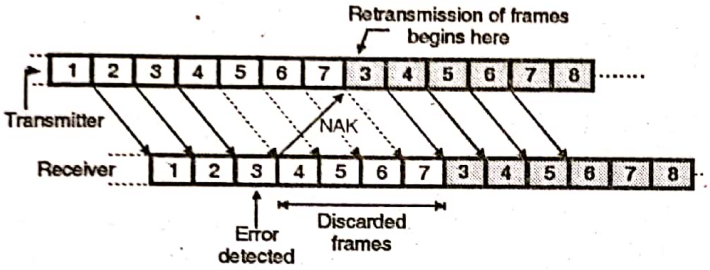
Ans. : In this stop and wait protocol it was assumed that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgement to come back is negligible. But in some practical situations, this assumption is not correct. In the systems like satellite system the round trip time can be as long as 500 mS (propagation delay). This will reduce the efficiency of the protocol. Therefore an improved protocol known as **GO-Back-n ARQ** has been developed.

Scanned by CamScanner

It is a method used to overcome the inefficiency of the stop and wait ARQ by allowing the transmitter to continue sending enough frames so that the channel is kept busy while the transmitter waits for acknowledgements. In this method if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.

Principle of GO-back-n ARQ :

Refer Fig. 3.10 to understand the principle of GO-Back-n ARQ.



(G-239)**Fig. 3.10 : Go back n ARQ system**

The sender does not wait for ACK signal for the transmission of next frame. It transmits the frames continuously as long as it does not receive the "NAK" signal. NAK is the negative acknowledgement signal sent by the receiver to the transmitter.

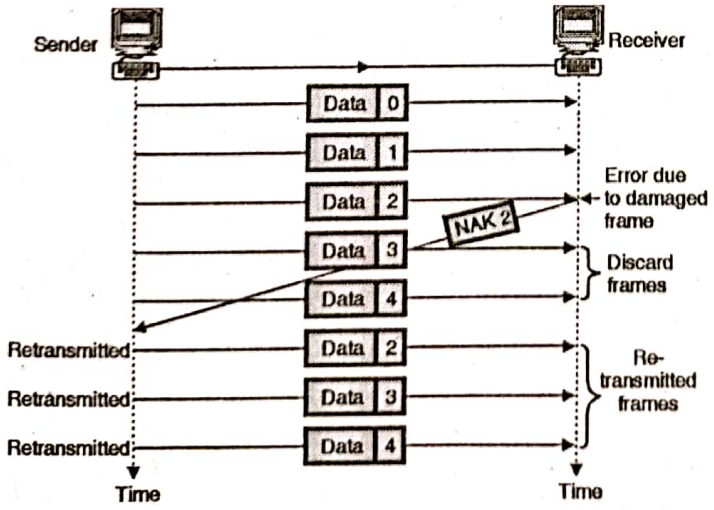
When the receiver detects an error in the third frame as shown in Fig. 3.10, the receiver sends a NAK signal back to sender. But this signal takes some time to reach the transmitter. By that time the transmitter has transmitted frames upto frame 7. On reception of the NAK signal, the transmitter will retransmit all the frames from 3 onwards. The receiver discards all the frames it has received after 3 i.e. 3 to 7. It will then receive all the frames that are retransmitted by the transmitter.

Sources of error :

The errors can get introduced, if the transmitted frames are damaged or lost or if the acknowledgement is lost. Now consider the operation of this protocol under these conditions.

Operation when the frame is lost :

This condition is illustrated in Fig. 3.10(a).



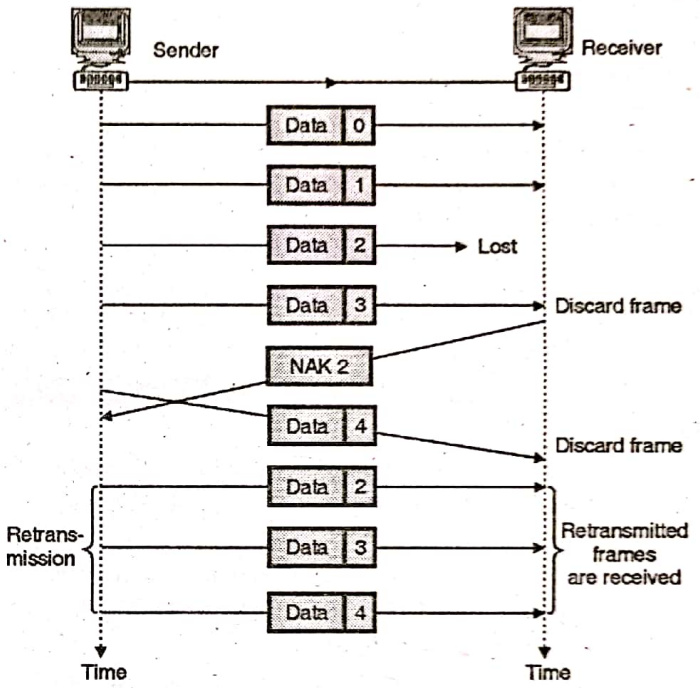
(G-240)**Fig. 3.10(a) : Go-back-n, damaged data frame**

The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back.

On receiving this signal, the transmitter starts retransmission from frame 2. All the frames received after frame 2 are discarded by the receiver.

Operation when a frame is lost :

As shown in Fig. 3.10(b) the case of lost frame is also treated in the same manner as that of the damaged frame.

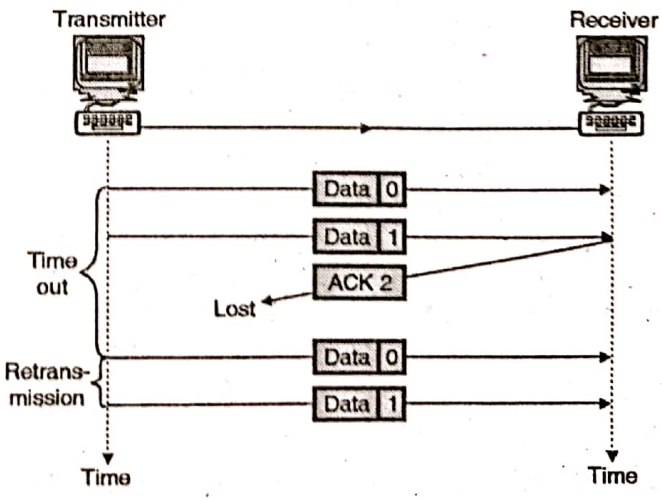


(G-241)**Fig. 3.10(b) : Go-back-n, lost data frame**

The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

Operation when the acknowledgement is lost :

Fig. 3.10(c) shows the condition for lost acknowledgement. In case of go-back-n method the transmitter does not expect an acknowledgement after every data frame.



(G-242)**Fig. 3.10(c) : Go-back-n, lost ACK frame**

Scanned by CamScanner

It cannot use the absence of sequential ACK numbers to identify lost ACK or NAK frames, instead it uses a timer. The transmitter can send as many frames as the window allows before waiting for an acknowledgement. Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the data frames again.

The disadvantage of Go-back-n ARQ protocol is that in noisy channels it has poor efficiency because of the need to retransmit the frame in error and all the subsequent frames.

Disadvantages of Go back n :

1. It transmits all the frames if one frame is damaged or lost.
2. It transmits frames continuously as long as it does not receive the NAK signal.
3. The NAK signal takes some time to reach the sender. Till that time the sender has already sent some frames. All those will be retransmitted after receiving the NAK.
4. The error can get introduced if the NAK is lost.

Q. 16 Explain sliding windows protocol with selective repeat.

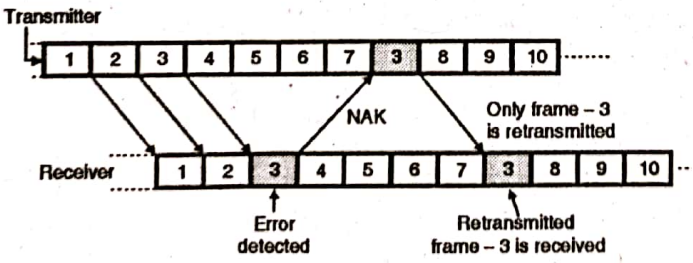
Dec. 03, May 13, Dec. 14, Dec. 15, May 17

Ans. :

In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways :

1. The receiver can do sorting of data frames and is also able to store frames received after it has sent the NAK until the damaged frame has been replaced.
2. The transmitter has a searching mechanism that allows it to choose only those frames which are requested for retransmission.
3. The window size in this method is less than or equal to $(n + 1)/2$, whereas in case of go-back-n it is $n - 1$.

The principle of operation of this protocol is illustrated in Fig. 3.11.



(G-243)**Fig. 3.11 : Selective repeat ARQ system**

In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next frame. It transmits the frames continuously till it receives the "NAK" signal from the receiver.

The receiver sends the "NAK" signal back to the transmitter as soon as it detects an error in the received frame. For example the receiver detects an error in the third frame, as shown in Fig. 3.11. By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 3.11. On reception of "NAK" signal, the transmitter will retransmit only the frame-3 and then continues with the sequence 8, 9... as shown in Fig. 3.11.

The frames 4, 5, 6 and 7 received by the receiver which do not contain any error are not discarded by the receiver. The receiver receives the retransmitted frames in between the regular frames. Therefore the receiver will have to maintain the frames sequentially.

Hence the selective repeat ARQ is the most efficient but the most complex protocol, of all the ARQ protocols.

Thus in selective repeat ARQ only the frame which is damaged or lost is retransmitted by the transmitter. The lost ACK or NAK frames are treated in the same manner as the go-back-n method. When the transmitter reaches either the capacity of its window $[(n + 1)/2]$ or the end of its transmission it sets a timer.

If no acknowledgement arrives in the allotted time, all the frames that remain unacknowledged are retransmitted. The disadvantage of this method is that because of the complexity of sorting and storage required by the receiver and the extra logic needed by the transmitter to select frames for retransmission, the system becomes more expensive. The advantage of this system is that it gives the best throughput efficiency. This is due to the use of pipelining in selective repeat ARQ.

Q. 17 Compare Stop and wait protocol, Go-back-n technique and Selective repeat ARQ. May 17

Ans. :

Table 3.1 : Comparison of sliding window protocols

Sr. No.	Parameter	Stop and wait	Go back n ARQ	Selective repeat ARQ
1.	Window size	1.	Sending window size : $(2^m - 1)$	Sending window size : 2^{m-1}
2.	Operating principle	Transmits one frame at a time and waits for its ACK signal. Transmits the next frame only if ACK is obtained.	It transmits frames continuously till it receives the NAK signal.	Same as Go back n protocol.
3.	Communication type (Direction wise).	Communication is one way (simplex) for the data frames though the ACK frames are allowed to travel in the opposite direction.	Communication is one way (simplex) for the data frames though the NAK frames are allowed to travel in the opposite direction.	Same as Go back n protocol
4.	Retransmission takes place if	1. Received frame is damaged.	1. Received frame is damaged.	Same as Go back n protocol

Scanned by CamScanner

Sr. No.	Parameter	Stop and wait	Go back n ARQ	Selective repeat ARQ
		2. Transmitted frame is lost 3. ACK is lost	2. Transmitted frame is lost. 3. NAK is lost.	
5.	Retransmission	Only the damaged or lost frame is retransmitted.	On reception of the NAK signal, the transmitter retransmits all the frames from the one for which the NAK is obtained.	On reception of NAK, only the damaged or lost frame is retransmitted.
6.	Principle of pipelining.	Not used	Used	Used.
7.	Efficiency	Least efficient and slow	Moderately efficient due to pipelining	Most efficient due to pipelining.
8.	Complexity	Less complex	Moderately complex.	Highly complex.

Q. 18 Explain HDLC protocol.

Dec. 07, May 08, May 11, Dec. 13, Dec. 16

Ans. :

The high level data link control (HDLC) protocol was developed by ISO. It is the most widely accepted data link layer protocol. It has the advantages of flexibility, adaptability, reliability and efficiency of operation. HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.

For the HDLC protocol the following three types of stations have been defined :

1. Primary station 2. Secondary station
3. Combined station

1. Primary station :

A primary station takes care of the data link management. When communication between the primary and secondary stations takes place, the primary station would connect and disconnect the data link. The frames sent by a primary station are called commands.

2. Secondary station :

A secondary station operates under the control of a primary station. When communication between primary and secondary stations takes place, the frames sent by the secondary station takes place are called responses.

3. Combined station :

A combined station can act as primary as well as secondary stations. Therefore it can send both commands and responses.

Operating modes for data transfer :

In HDLC both synchronous and asynchronous modes of communication are permitted.

The meaning of the words synchronous and asynchronous is different from that of a physical layer. Following modes of operation are possible for data transfer :

1. Normal response mode (NRM)
2. Asynchronous response mode (ARM)
3. Asynchronous balanced mode (ABM)

The first two modes of operation are suitable for an unbalanced type of data transfer between one primary and the other secondary stations whereas the third one is suitable for a balanced type of data transfer.

Normal Response Mode (NRM) :

This mode is suitable for point-to-point as well as point-to-multipoint configurations. Here the primary station will control the overall data link management. It is a synchronous mode of communication.

Asynchronous Response Mode (ARM) :

This mode is used for communication between primary and secondary stations. As the name indicates it is an asynchronous mode of communication.

In ARM the secondary station can transmit response (frame) without taking permission from the primary station. This is not allowed in NRM. Therefore NRM is a more disciplined mode than ARM. The responsibility of link management function still lies with the primary station.

Asynchronous Balanced Mode (ABM) :

This mode is applicable to the point to point communication between two combined station. As both these stations are combined stations, they are capable of link management functions. As the communication is asynchronous, one station can transmit a frame without permission from the other station. In this mode information frames can be transmitted in full duplex manner.

Q. 19 Explain the frame formats of HDLC I-frame, U-frame and S-frame. Dec. 07

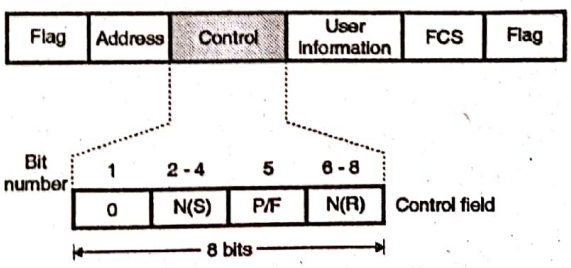
Ans. :

There are three types of frames defined in HDLC as follows :

1. The I-frame or information frame.
2. The S-frame or supervisory frame.
3. The U-frame or the unnumbered frame.

The I-frame :

Fig. 3.12 shows the format of the information frame or I-frame.



(G-251)**Fig. 3.12 : I-frame format**

Scanned by CamScanner

It is supposed to carry the user data from the network layer. It is also possible to include the flow and error control information which is also called piggybacking.

Explanation :

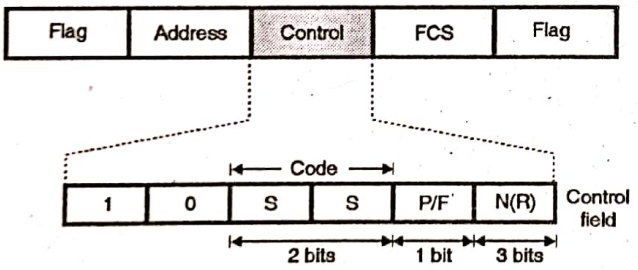
Concentrate on the control field of the I-frame. As shown in the Fig. 3.12 if the first bit in the control field is 0 it is identified as an information frame (I-frame). The next three bits (2 to 4) are called N (S) and their job is to define the sequence number of the frame. Since there are only 3 bits, we can define only eight combinations ($2^3 = 8$). Therefore a sequence number is between 0 and 7 only. The value of N(S) field corresponds to the value of control variable S for the three ARQ mechanisms.

The next bit (5^{th}) is the poll/final (P/F) bit. It can have two possible values 0 or 1 out of which only the logical 1 is meaningful. Logic 0 in this position has no meaning. When P/F = 1, it means poll when a frame is sent by a primary station to secondary. . When P/F = 1, it means final when a frame is sent by a secondary station to primary.

The last three bits (6 to 8) define the N(R) field. It is used for piggybacking. The 3 bits in the N(R) field will represent the value of ACK when piggybacking is used.

The S-Frames :

Fig. 3.12(a) shows the format of S-frames or supervisory frames. An S-frame does not contain any information field. These frames are used for flow and error control when piggybacking is not possible to implement or when piggybacking is not appropriate to implement.



(G-252)**Fig. 3.12(a) : S-frame format**

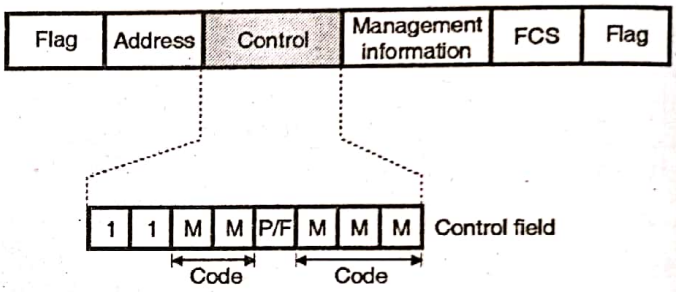
Refer to the control field of the S-frame. A 10 in the first two bits of the control field identifies it as a Supervisory frame or S-frame as shown in Fig. 3.12(a). The next two bits define the code field marked SS. There are four possible combinations of these bits. They indicate different types of S-frames. There are 4 types of supervisory frames corresponding to the four possible value of the S bits in the control field.

1. SS = 00 → corresponds to receive ready (RR) frames which are used to acknowledge frames when no I frames are available to piggyback the acknowledgement.
2. SS = 01 → corresponds to Reject (REJ) frames which are used by the receiver to send a NAK when error has occurred.
3. SS = 10 → corresponds to a Receive Not Ready (RNR) frame and it is used for flow control.
4. SS = 11 → corresponds to a Selective Repeat Frame which indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.

The fifth bit in the control field is P/F bit the function, and the next 3 bits called N(R) correspond to the ACK or NAK value.

U-frames :

The format of U-frame i.e. the unnumbered frame is shown in Fig. 3.12(b). These frames are used for exchanging the session management and control information between the communicating devices.



(G-253)**Fig. 3.12(b) : Format of U-frame**

A 11 in the first two bits of the control field identifies an unnumbered (U) frame as shown in Fig. 3.12(b). The information field in U-frame is used for carrying the system management information. It does not carry the user data. The U-frame code bits (M bits in Fig. 3.12(b)) are divided into two sections. Two bits before P/F bit and three bits after the P/F bits. These five code bits can create upto $2^5 = 32$ different types of U-frames. The unnumbered frame types are used for functions such as initialization, status reporting and resetting. The Information frame and supervisory frames implement the error and flow control functions of the data link layer. The combination of the I-frames and supervisory frames allows HDLC to implement stop-and-wait, Go-back-n and selective repeat ARQ.

Q. 20 Why does the data link protocol always put the CRC in a trailer rather than in a header ?

May 15

Ans. :

Note that for all the data link protocols so far, the CRC field that contains the checksum for error detection and correction, always appears in the trailer i.e. at the end of the frame and not in the header.

The CRC is obtained by adding all the bits being transmitted, and appended to the outgoing stream as soon as the last bit is transmitted. If we want CRC to be in the header i.e. at the beginning of the frame, then the CRC has to be calculated by scanning the frame before transmission. This would require each byte to be handled twice, once for computing CRC and then for transmission. But if CRC is put in the trailer, then each byte will have to be handled only once.

Scanned by CamScanner

Q. 21 Consider a message represented by the polynomial $M(x) = x^5 + x^4 + x$. Consider a generating polynomial $G(x) = x^3 + x^2 + 1$ (1101). Generate a 3 bit CRC and show what will be the transmitted frame. How is error detected by CRC ? May 17

Ans. :

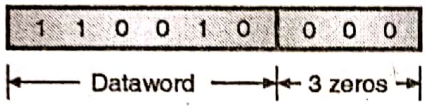
Given : Data word : $x^5 + x^4 + x = 110010$

Generator polynomial : $x^3 + x^2 + 1 = 1101$

Step 1 : Obtain the dividend :

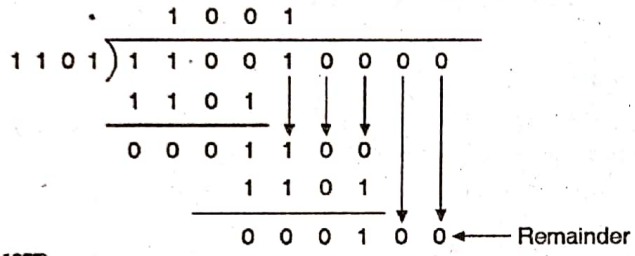
Dividend = Dataword + 3 zeros.

The dividend is as follows :



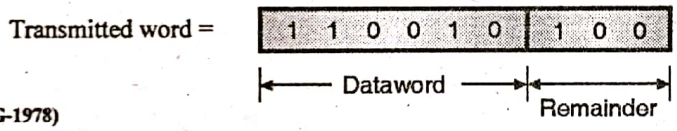
(G-1976)

Step 2 : Carry out the division :



(G-1977)

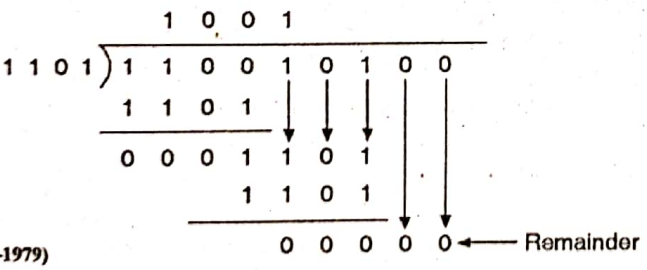
Step 3 : Obtain the transmitted frame :



(G-1978)

Error detection :

At the receiver, this word is divided by the same divider used at the transmitter i.e. 1101.



(G-1979)

A zero remainder indicates that there is no error in the received codeword.

Q. 22 Write short notes on : Point-to-Point Protocol (PPP). Dec. 09

Ans. :

One of the most common protocols used for point to point access is PPP. The long form of PPP is point to point protocol. This protocol is used by a lot of Internet users to connect their home computers to the server of an Internet service provider (ISP).

Most of these users have a traditional modem and they are connected to the Internet through a telephone line or a TV cable. The PPP is used for controlling and managing the data transfer.

Services Provided by PPP :

Following are some of the services provided by PPP :

1. To define the frame format.
2. It defines how the link between two devices is to be established and how the data exchange should take place.
3. It decides the encapsulation of network layer data into the data link frame.
4. It defines the way in which the two devices can authenticate each other.

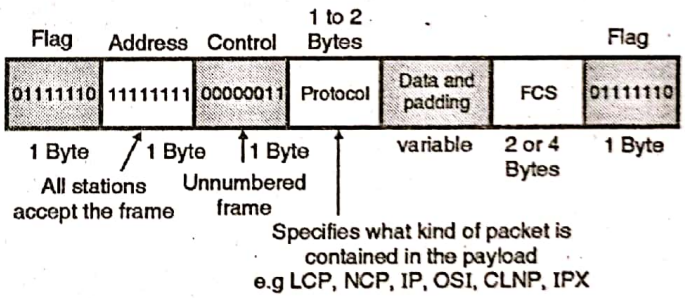
This protocol was designed for users who wanted to connect their computer system through a telephone line to the computer of an Internet service provider to access internet.

The PPP protocol can operate over a variety of point to point transmission links such as ADSL and SONET. The PPP was an improvement over the Serial Line Internet Protocol (SLIP).

Q. 23 Write in brief about : PPP frame format. Dec. 15

Ans. :

The PPP protocol uses an HDLC like frame format as shown in Fig. 3.13.



(G-256)**Fig. 3.13 : Frame format of PPP**

The descriptions of various fields is as follows :

1. **Flag :** The PPP frame always begins and ends with the standard HDLC flag i.e. 01111110.
2. **Address :** Since PPP is used for a point-to-point connection, it uses the broadcast address of HDLC i.e. 11111111, to avoid a data link address in the protocol. All 1's in the address field indicates that all stations are to accept the frame.
3. **Control :** This field has the same format as that of the U-frame in HDLC. The value is 00000011 in this field indicates that the frame does not contain any sequence numbers and that there is no flow or error control.
4. **Protocol :** It defines the nature of contents of the data field, i.e. user data or other information.
5. **Data field :** It carries either the user data or other information.

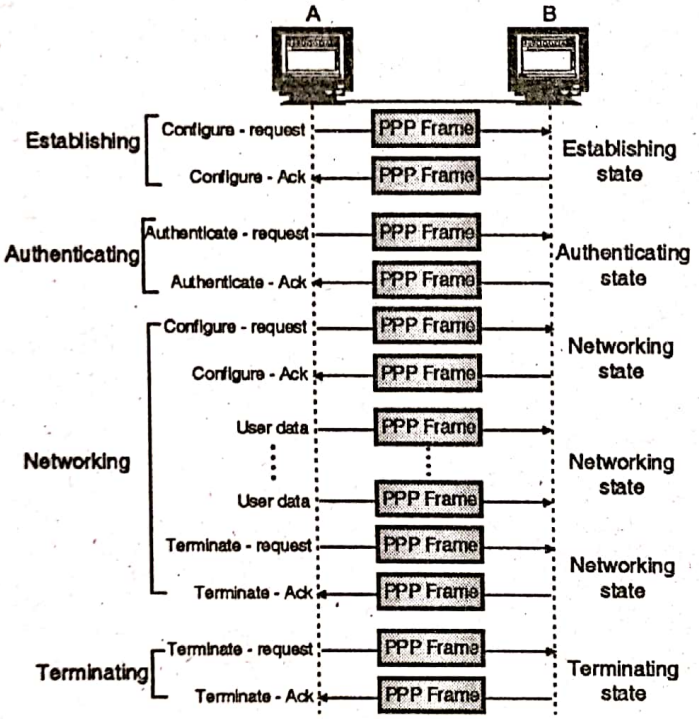
Scanned by CamScanner

6. **FCS (Frame Check Field) :** This field is a 2 or 4 byte CRC. It can use the CCITT 16 or CCITT 32 generator polynomial.

The PPP protocol provides many useful capabilities if used alongwith two protocols namely a Link Control Protocol (LCP) and the Network Control Protocol (NCP).

The Link Control Protocol (LCP) is used to carry out various tasks such as to set-up, configure, test, maintain and terminate a link connection. After authentication has been completed a Network Control Protocol (NCP) is used. The NCP consists of multiple control protocols. It help in the encapsulation of data coming from network layer protocols such-as IP, IPX, Decent, Apple Talk in the PPP frame.

The PPP connection will have to go through different states, such as establishing authenticating, networking and terminating state as shown in Fig. 3.13(a).

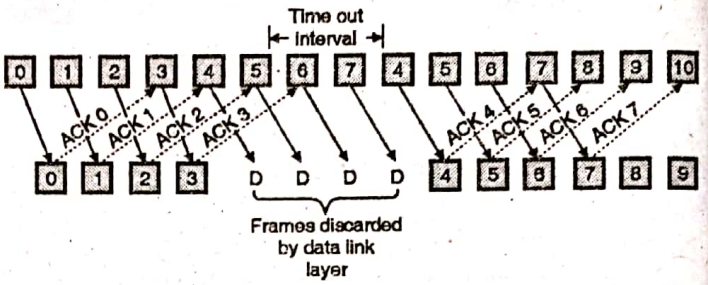


(G-257)**Fig. 3.13(a) : States of PPP connection**

Q. 24 Draw the sender and receiver windows for a system using Go-Back-N sliding window system given that

1. **Frame 0 is sent ; Frame 0 is ACK**
2. **Frames 1 and 2 are sent ; Frames 1 and 2 are ACK.**
3. **Frames 3, 4, 5 are sent. Frame 4 is ACK. Timer for frame 5 expires.**
4. **Frames 5, 6, 7 are sent, Frames 4 through 7 are ACK.** Dec. 04, Dec. 13

Ans. :



(G-803) **Fig. 3.14 : Go-Back-N sliding window**

Q. 25 What are the advantages of a variable length frame over fixed length frames ? May 12, May 13

Ans. :

The data link layer packs bits into frames so that each frame is distinguishable from the other frames.

Framing can be of two different types :

1. Fixed size framing
2. Variable size framing.

In the fixed size framing, the frame size is fixed. It is same for all frames. Hence there is no need for defining the boundaries of the frames. This type of framing is used in ATM wide area networks. The variable size framing is used in LANs. In this type of framing it is necessary to define the end of a frame and beginning of next frame.

Advantages of variable size framing :

1. Although the whole message could be packed in one big frame, it is not done practically because for large frames the flow and error control becomes inefficient. Also even for a single error the whole message needs to be retransmitted. When the same message is divided into smaller frames, the flow and error control become efficient.
2. In LANs there are more than one senders. The messages sent by them could be of different size. Hence it makes system efficient by keeping frame size variable as it is possible to select an optimum frame size as per requirements.

Chapter 4 : Medium Access Control Layer & LAN

Q. 1 Write short notes on : ALOHA. Dec. 06, May 10, Dec. 10, May 11, May 13

Ans. : ALOHA System :

Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as Contention systems.

The ALOHA system is a contention protocol which was developed at the University of Hawaii in the early 1970's by Norman Abramson and his colleagues. The ALOHA system has two versions :

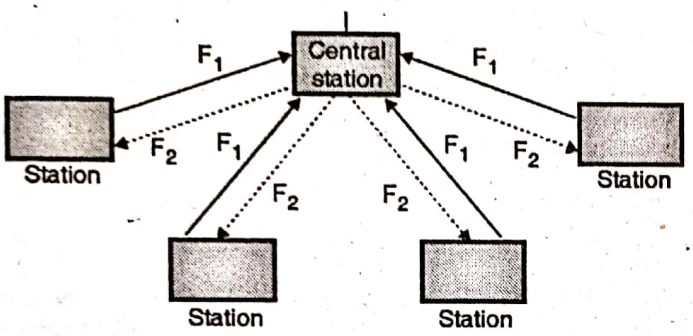
1. Pure ALOHA – Does not require global time synchronisation.
2. Slotted ALOHA – Requires time synchronisation.

Scanned by CamScanner

Pure ALOHA :

It works on a very simple principle. Essentially it allows for any station to broadcast at any time. If two signals collide, each station simply waits a random time and try again.

Collisions are easily detected. As shown in the Fig. 4.1, when the central station receives a frame it sends an acknowledgement on a different frequency.



F_1 = Broadcast frequency from the individual stations.

F_2 = Broadcast frequency from the central station.

(G-268)**Fig. 4.1 : Pure ALOHA system**

If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does get an acknowledgement it assumes that collision had occurred and is ready to retransmit. The advantage of pure ALOHA is its simplicity in implementation but it's performance becomes worse as the data traffic on the channel increases.

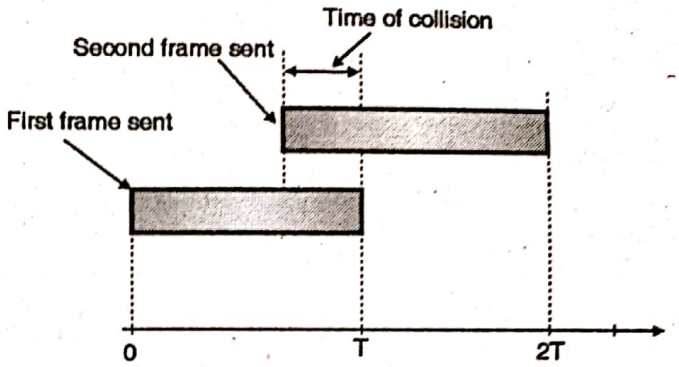
Q. 2 Describe in brief : Slotted ALOHA.

Dec. 07, May 10, Dec. 16

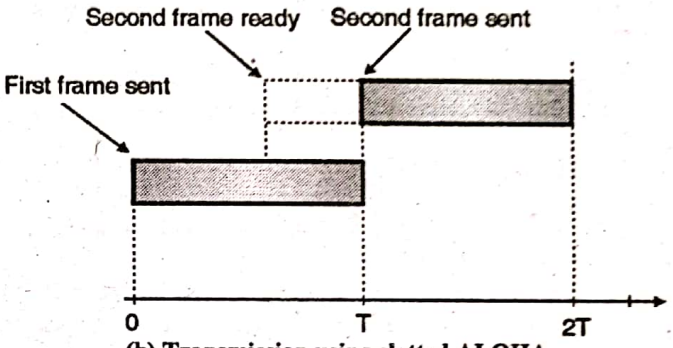
Ans. :

To overcome the disadvantage of the pure ALOHA system (of low capacity) Robert published a method for doubling the capacity of traffic on the channel. In this method it was proposed that the time be divided up into discrete intervals and each interval correspond to one frame. This method requires that the users agree on the slot boundaries. In this method for achieving synchronization one special station emits a pip at the start of each interval, like a clock. This method is known as the slotted ALOHA system.

Collisions occur if any part of two transmission overlaps. Suppose that T is time required for one transmission and that two stations must transmit. The total time required for both stations to do so successfully is 2T as shown in Fig. 4.2. In case of pure ALOHA allowing a station to transmit at arbitrary times can waste time upto 2T.



(a) Transmission using pure ALOHA



(b) Transmission using slotted ALOHA

(G-271)**Fig. 4.2**

As an alternative, in the slotted ALOHA method the time is divided into intervals (slots) of T units each and require each station to begin each transmission at the beginning of a slot.

In other words, even if station is ready to send in the middle of a slot, it must wait until the beginning of the next one as shown in Fig. 4.2(b). In this method a collision occurs when both stations become ready in the same slot. Slotted ALOHA is thus a discrete time system whereas pure ALOHA is a continuous time system. The Vulnerable period has been reduced to half that of pure ALOHA, the throughput for slotted ALOHA is given by,

$$S = Ge^{-G}$$

The maximum throughput corresponds to G = 1 and it is given by $S_{max} = 1/e = 0.368$. So for a slotted ALOHA with G = 1 the probability of success is 37%. The probability of empty slots is,

$$P(k) = \frac{G^k e^{-G}}{k!}$$

For G = 1 and k = 0 we get P (k = 0) = 0.368.

And the probability of collisions is 26 %.

The probability of transmission requiring exactly k attempts (i.e. k – 1 collisions followed by one success) is given by,

$$P_k = e^{-G}(1 - e^{-G})^{k-1}$$

And the expected number of transmissions E per carriage return typed is

$$E = e^{G}$$

Conclusion : As E depends exponentially on G, with a small increase in G, there is a large increase in E and drastic fall in performance.

Scanned by CamScanner

Q. 3 Derive the efficiency of Pure ALOHA protocol.

Dec. 04, May 12, Dec. 16

Ans. :

Efficiency of an ALOHA system is that fraction of all transmitted frames which escape collisions i.e. which do not get caught in collisions.

Consider ∞ number of interactive users at their computers (stations). Each user is either typing or waiting. Initially all of them are in the typing state. When a user types a line, the user stops and waits. The station then transmits a frame containing this line and checks the channel to confirm the success. If it is successful then the user will start typing again, otherwise the user waits and its frame is retransmitted many time till it is sent successfully.

Frame time :

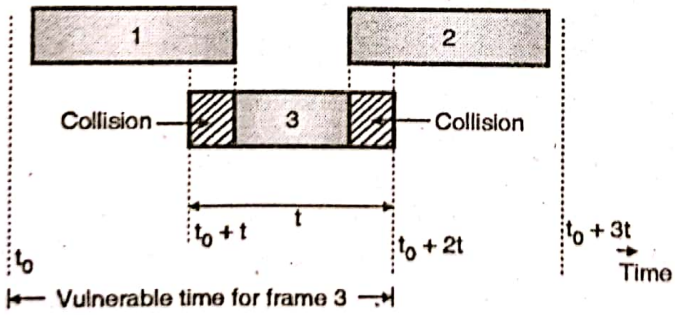
Let the frame time be defined as the amount of time required to transmit the standard fixed length frame. Note that

$$\text{Frame time} = \frac{\text{Frame length}}{\text{Bit rate}}$$

We assume that ∞ number of users generate new frames according to the Poisson's distribution with an average N frames per frame time. The value of $N > 1$ indicates that the users are generating frames at a rate higher than that can be handled by the channel. So most of the frames will face collision. Hence $0 < N < 1$ in order to reduce number of collisions. Let there be k transmission attempts (including retransmissions) per frame time. The probability of k transmissions per frame time is also Poisson. Let the mean of number of transmissions be G per frame time. So $G \geq N$. At low load $N \approx 0$ there will be less number of collisions so less number of retransmissions and $G \approx N$. With increase in load there are many collisions so $G > N$. Combining all these we can say that for all the loads the throughput is given by,

$$S = GP_0$$

Where P_0 = Probability that a frame does not suffer a collision. Consider Fig. 4.3.



(G-270) **Fig. 4.3**

What is the condition for frame 3 in Fig. 4.3 to arrive undamaged without collision ? Let t = time required to send a frame. If frame 1 is generated at any instant between t_0 to $(t_0 + t)$ then it will collide with frame 3. Similarly any frame (2) generated between $(t_0 + t)$ and $(t_0 + 2t)$ also collides with frame 3. As per Poisson's distribution, the probability of generating k frames during a given frame time is given by,

$$P[k] = \frac{G^k e^{-G}}{k!}$$

So the probability of generating zero frames i.e. $k = 0$ is

$$P_0 = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

If an interval is two frame time long, the mean number of frames generated during that interval is 2G. The probability that no other frame is transmitted during the Vulnerable period (time when collision can take place) is,

$$P_0 = e^{-2G}$$

But throughput $S = G P_0$

$$\therefore \quad S = Ge^{-2G}$$

Fig. 4.4 shows the relation between the offered traffic G and the throughput S. It shows that the maximum throughput occurs at $G = 0.5$ and $S_{max} = 0.184$. So the best possible channel utilization is on 18.4 percent.

Q. 4 Differentiate between ALOHA and slotted ALOHA.

May 13, May 15

Ans. :

A mathematical model can be created for the relationship between the number of frames transmitted and the number of frames transmitted successfully. Let G represent the traffic measured as the average number of frames generated per slot. Let S be the success rate measured as the average number of frames sent successfully per slot.

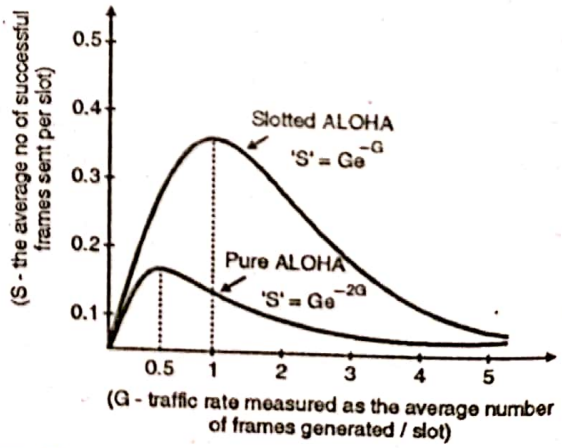
The relationship between G and S for both pure and slotted ALOHA is given as follows :

Pure ALOHA $\rightarrow S = Ge^{-2G}$

Slotted ALOHA $\rightarrow S = Ge^{-G}$

Where e is the mathematical constant = 2.718.

From the above equation a success rate curve for pure and slotted ALOHA can be plotted as shown in Fig. 4.4. As seen in the Fig. 4.4 both graphs have the same shape. If G is small so is S, which means that if few frames are generated few frames will be transmitted successfully. As G increases so does S but upto a certain point. As G continues to increase S approaches to 0 which means that if more frames are generated there will be more collisions and the success rate will fall to 0.



(G-272) **Fig. 4.4 : Comparison of pure and slotted ALOHA**

Scanned by CamScanner

Similarly for pure ALOHA the maximum occurs at G = 0.5 for which S = 1/2e = 0.184 which means the rate of successful transmissions is approximately 18.4%. As seen from the graph the maximum for slotted ALOHA occurs at G = 1 for which S = 1/e = 0.368. In other words the rate of successful transmissions is approximately 0.368 frames per slot time or 37% of the time will be spent on successful transmissions.

Hence the slotted ALOHA has a double throughput efficiency than the pure ALOHA system. The maximum utilization achievable using CSMA can be increased much beyond that obtainable using ALOHA or slotted ALOHA. The maximum utilization is dependent on length of the frame and on the propagation time. With increase in the length of the frame or reduction in the propagation time the utilization gets improved.

Q. 5 Explain CSMA protocols.

Dec. 04, Dec. 13, Dec. 14, May 15, Dec. 16, Dec. 17

Ans. :

The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-Persistent CSMA :

In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time. After this time, it again checks the status of the channel and if the channel is free it will transmit.

1-Persistent CSMA :

In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately. The disadvantage of this strategy is that if two stations are waiting then they will transmit simultaneously and collision will take place. This will then require retransmission.

P-Persistent CSMA :

The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle. A station is assumed to be transmitting with a probability "p". For example if p = 1/6 and if 6 stations are waiting then on an average only one station will transmit and others will wait.

Q. 6 Write in brief about : CSMA/CD

Dec. 13, Dec. 14, May 15, Dec. 15, Dec. 16, Dec. 17

Ans. :

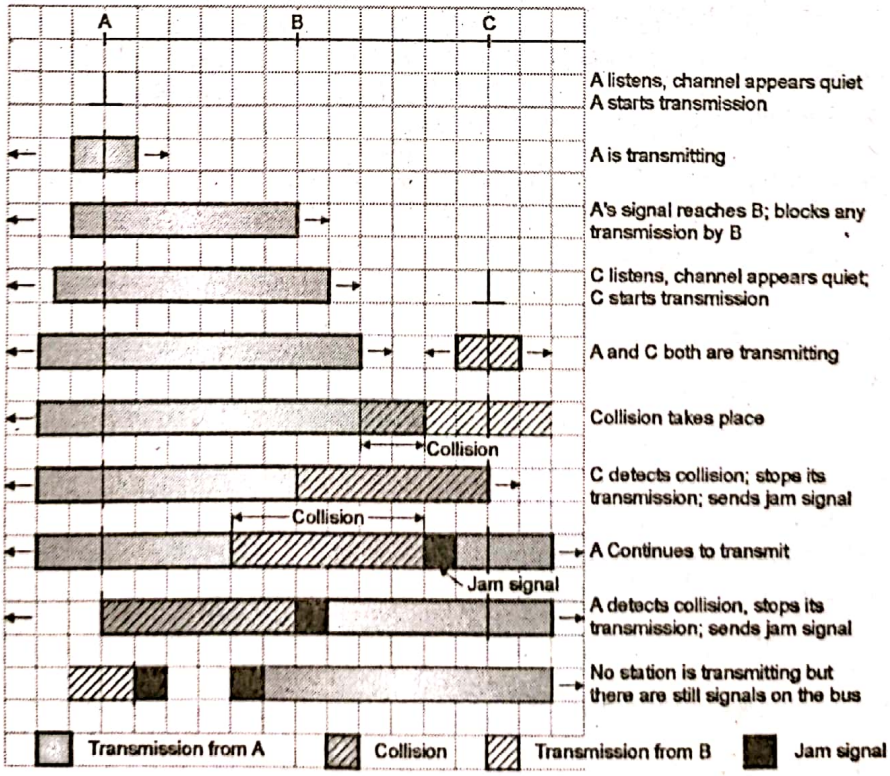
The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

The problem in CSMA is that a transmitting station continues to transmit its frame even though a collision occurs. The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.

As soon as a collision is detected, the transmitting stations release a jam signal.

The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.

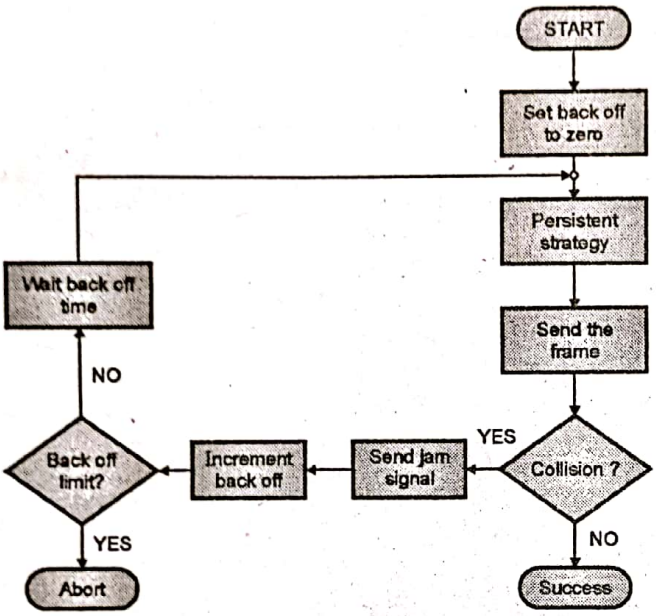


(G-273)Fig. 4.5 : CSMA/CD scheme

Scanned by CamScanner

Otherwise there is a possibility that the same frames would collide again. After some "back off" delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively. A careful design can achieve efficiencies of more than 90% using CSMA/CD. This scheme is as shown in Fig. 4.5.

Fig. 4.5(a) shows a flow chart for the CSMA/CD protocol.



(G-276)**Fig. 4.5(a) : CSMA/CD procedure**

Explanation :

The station that has a ready frame sets the back off parameter to zero.

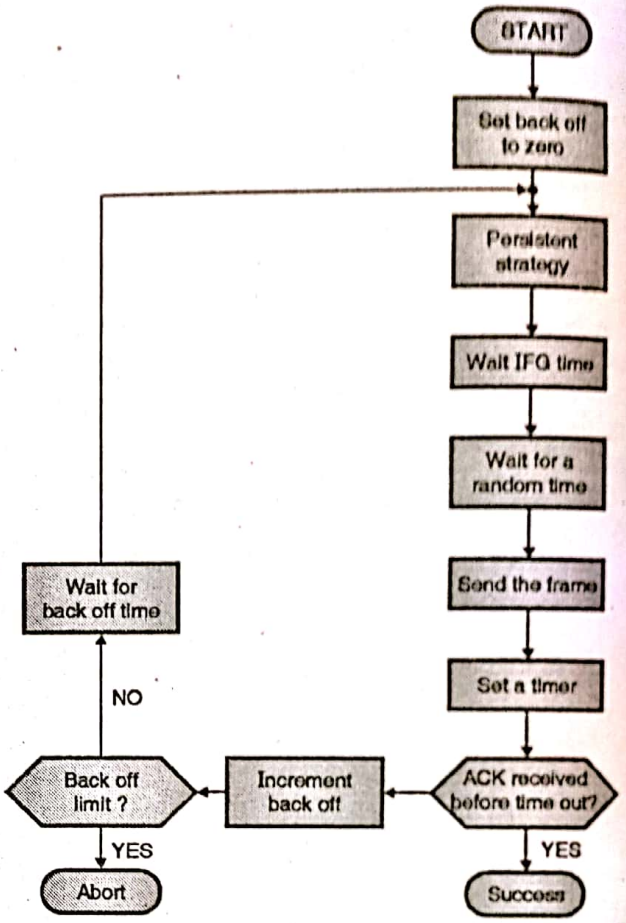
Then it senses the line using one of the persistent strategies. It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful. Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision. The station then increments the back off time and waits for a random back off time and sends the frame again.

If the back off has reached its limit then the station aborts the transmission. CSMA/CD is used for the traditional Ethernet. CSMA/CD is an important protocol. IEEE 802.3 (Ethernet) is an example of CSMA/CD. It is an international standard. The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

Q. 7 What is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol ? Explain with timing diagram. Dec. 09, Dec. 13

Ans. :

The long form of CSMA/CA is CSMA protocol with collision avoidance. Fig. 4.6 shows the flow chart explaining the principle of CSMA/CA.



(G-277)**Fig. 4.6 : CSMA/CA procedure**

The station ready to transmit, senses the line by using one of the persistent strategies.

As soon as it find the line to be idle, the station waits for a time equal to an IFG (Interframe gap). It then waits for some more random time and sends the frame. After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

If the acknowledgement is received before expiry of the timer, then the transmission is successful. But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and senses the line again. CSMA/CA completely avoids the collision.

Q. 8 What is controlled access for collision control ? Explain all the methods of controlled access. Dec. 15

Ans. :

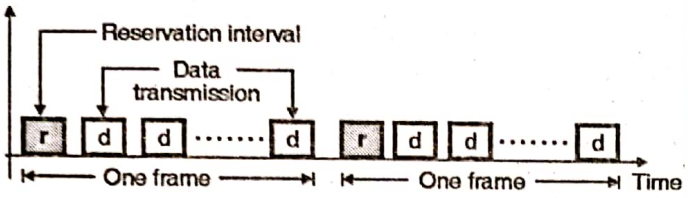
The random access approach is simpler to implement and are useful in handling the light traffic. Here we will see the scheduling approaches to the medium access control. There are three important approaches in the scheduling approach as follows :

1. Reservation system
2. Polling system
3. Token passing ring networks.

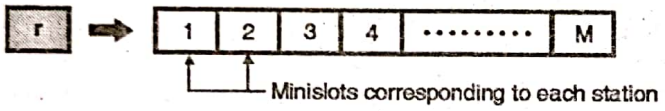
Scanned by CamScanner

Reservation Systems :

The principle of reservation system can be understood from Fig. 4.7. In this system each station transmits a single packet at the full rate R bps. The transmissions from the stations can be organized into frames of variable length. Before each frame a reserved slot or reservation interval is transmitted as shown in Fig. 4.7(a).



(a) Transmission in reservation systems



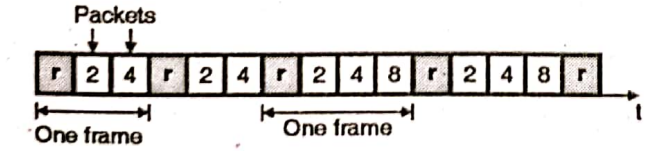
(b) Details of reservation interval

(L-733)Fig. 4.7 : Basic reservation system

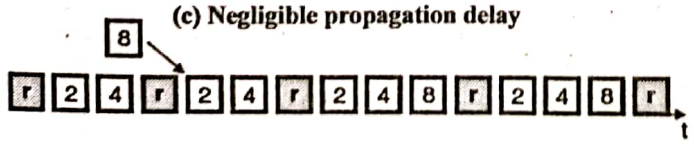
Fig. 4.7(b) shows the details of the reservation interval "r". The reservation interval consists of M minislots with one slot allotted to each station. These minislots are used by the stations to indicate that they have a packet to transmit in the corresponding frame. The station that wants to transmit packet by broadcasting their reservation bit during the appropriate minislot. All the stations will listen to the reservation interval, and then determine the order in which packet transmissions in the corresponding frame would take place. The frame length would correspond to the number of stations which have a packet to transmit.

If the length of the packet is variable, then it can be handled if the reservation message includes packet length information. This reservation system is called as the basic reservation system.

The basic reservation system can be improved by using the time division multiplexing scheme. In the improved reservation system the idle time slots are allotted to the other stations. The operation of the basic reservation system can be explained with the help of Fig. 4.7.



(c) Negligible propagation delay



(d) Non negligible propagation delay

(L-734)Fig. 4.7 : Operation of reservation system with negligible and non-negligible delays

Refer Fig. 4.7(c) which shows a system with negligible propagation delay. In the first frame, only the stations 2 and 4 transmit their packets. But in the middle portion, station 8 also wants to transmit its packet. So the frame gets expanded from two slots to three slots. The maximum throughput from this system can be attained when all the stations transmit their packet in each frame. The corresponding maximum throughput is given by,

$$\rho_{max} = \frac{1}{1+v} \quad \text{...for one packet reservation/minislot}$$

If $v << 1$ then the value of ρ_{max} can be very high.

Now refer Fig. 4.7(d) which shows a reservation system with some finite non zero propagation delay which cannot be neglected. In this system the stations will transmit their reservations in the same way as they used to do before. It is possible to modify the basic reservation system so that stations can reserve more than one slot per packet transmission per minislot. Assume that a minislot can reserve say upto k packets.

Then the maximum achievable throughput is given by,

$$\rho_{max} = \frac{1}{1+(v/k)} \quad \text{...for k packet reservation/minislot}$$

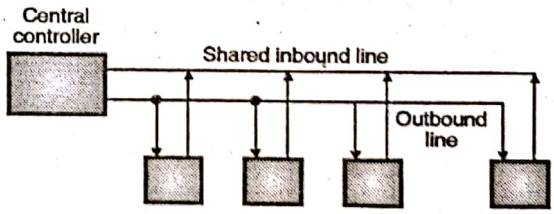
Note that this value of ρ_{max} will be higher than that for the single packet reservation/minislot.

Effect of number of stations (M) :

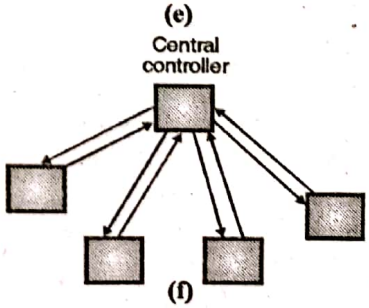
The reservation intervals introduce overhead which is proportional to M. That means the reservation interval becomes M × v. As the number of stations (M) become very large, this overhead will become significant. This then becomes a serious problem. This problem can be sorted out by not allocating a minislot to each station and then instead making the stations to compete for a reservation of minislot by using a random access technique such as ALOHA or slotted ALOHA.

Polling :

Now consider polling system shown in Fig. 4.7. In this system the stations access the common medium one by one (by taking turns). At any given time only one of the stations will transmit into the medium.



(e)



(f)

(L-735)Fig. 4.7 : Examples of polling systems

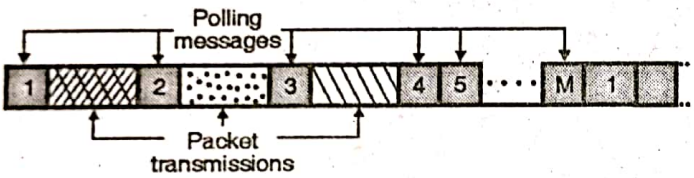
Scanned by CamScanner

When a station finishes its transmitting, then some mechanism is used to pass the right of transmission to another station which wants to transmit next. There are different ways of passing the right of transmission from one station to the other station. Fig. 4.7(e) shows a scheme in which M stations communicate with a central controller. The outbound line is used for carrying the information from the central controller to the M users whereas the shared inbound line is required to carry the information from users to the central computer. Thus the inbound line acts as the shared medium that requires a medium access control (MAC).

The host computer acts as a central controller. It sends control messages which co-ordinate the transmissions from the stations. The central controller sends a polling message to a particular station. That station sends its message on the shared inbound line. Once this process is over, the station gives a go-ahead message.

It is possible that the central controller may poll the stations in a round robin (serial) fashion or it may do it according to some pre-determined rule. Fig. 4.7(f) shows another system where it is possible to use polling. The central controller of this system can make use of radio transmission.

Fig. 4.7(g) shows the sequence of polling messages.



(L-736)**Fig. 4.7(g) : Polling messages and transmissions in a polling system**

Station 1 gets the polling message first. The polling message will propagate. It is received by all stations but only station 1 begins transmission. All this process needs a time called **walk time.**

The next period is occupied by the transmission from station 1. This period will then be followed by the walk time corresponding to station-2. This process will continue until all the M stations are polled. Thus in this system the stations are polled in the round robin manner.

The walk time can be considered to be an overhead in the polling system because it is an unproductive time. The total walk time τ' is the sum of walk time corresponding to each station.

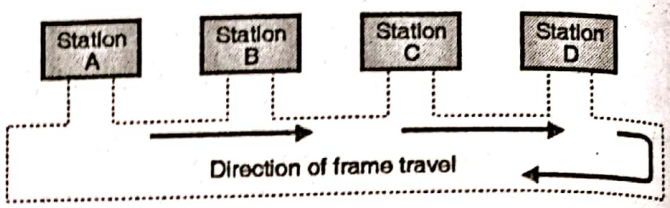
Q. 9 What is controlled access for collision control ? Explain all the methods of controlled access.

Dec. 15

Ans. :

Token is a special frame which is used to authorize a particular station for transmission.

In the token passing method, the token is given to that station, which is authorized to send its data. Thus the station that has the token with it can transmit others listen.



(L-737)**Fig. 4.8 : Token passing network**

In a token passing network, each station has a predecessor and successor as shown in Fig. 4.8. The frames travel in one direction. They come from the predecessor and go to the successor as shown in Fig. 4.8.

A token frame is circulated around the ring when no data is being transmitted and the line is idle. The stations which are ready to send data, will wait for the token. As the token circulates the first ready station in the ring will grab the circulating token and transmit one or more frames. This station will keep sending the frames as long as it has frames to send or the allotted time is not complete. It then passes this token on the ring from which the next ready to transmit station will grab it. This is the simplest possible token passing technique in which all the stations have equal priority or right to send. In the practical system, some other features such as priority and reservation are added.

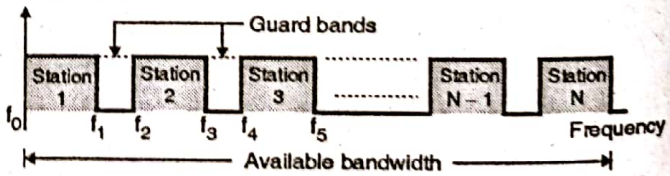
Q. 10 Explain FDMA, TDMA and CDMA.

May 12, Dec. 12, May 13

Ans. :

FDMA :

In the frequency division multiple access (FDMA), the available channel (medium) bandwidth is shared by all the stations. That means each station will have its own specific slot reserved in the entire channel bandwidth. So each station uses its allocated frequency band to send its data. Each band is thus reserved for a specific station. e.g. the frequency band f_0 to f_1 is for station-1, then f_2 to f_3 is for station-2 and so on. The concept of FDMA is illustrated is Fig. 4.9. FDMA is a data link layer protocol which uses FDM at the physical layer.



(L-739)**Fig. 4.9 : Concept of FDMA**

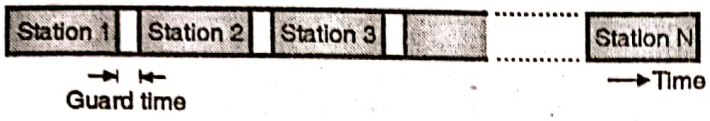
Guard bands are provided in between the adjacent frequency slots. e.g. $(f_1 - f_2)$ is a guard band between the bands allotted to stations 1 and 2. Guard bands avoid the adjacent channel interference. FDMA is used in cellular phones and satellite networks.

TDMA :

TDMA stands for Time Division Multiple Access. In TDMA, the entire bandwidth can be used by every user (station) but not simultaneously.

Scanned by CamScanner

A station can use the entire bandwidth only for the allocated time slot. Thus each channel is allocated a time slot only during which it can send its data. Thus the time is shared, frequency band is not shared. Fig. 4.9(a) illustrates the concept of TDMA. Guard times are inserted between the adjacent time slots in order to prevent any cross talk. No data transmission takes place during the guard times.



(L-740)**Fig. 4.9(a) : Concept of TDMA**

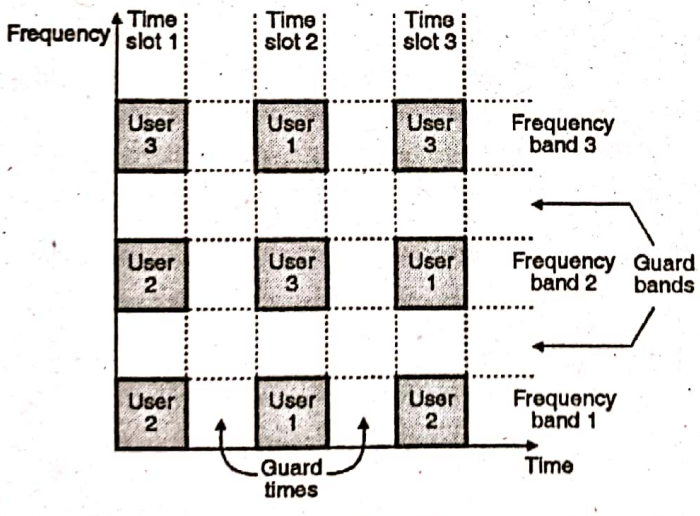
TDMA is a data link layer protocol which uses TDM at the physical layer. TDMA finds its application in cellular phones and satellite networks.

Code Division Multiple Access (CDMA) :

An alternative to FDMA and TDMA is an another system called code division multiple access (CDMA). The most important feature of CDMA is as follows :

In CDMA more than one user is allowed to share a channel or subchannel with the help of direct-sequence spread spectrum (DS-SS) signals.

In CDMA each user is given a unique code sequence or signature sequence. This sequence allows the user to spread the information signal across the assigned frequency band. At the receiver the signal is recovered by using the same code sequence. At the receiver, the signals received from various users are separated by checking the cross-correlation of the received signal with each possible user signature sequence.



(L-741)**Fig. 4.9(b) : Structure of CDMA showing the guard bands and the guard times**

In CDMA the users access the channel in a random manner. Hence the signals transmitted by multiple users will completely overlap both in time and in frequency.

The CDMA signals are spread in frequency. Therefore the demodulation and separation of these signals at the receiver can be achieved by using the pseudorandom code sequence.

CDMA is sometimes also called as spread spectrum multiple access (SSMA). In CDMA as the bandwidth as well as time of the channel is being shared by the users, it is necessary to introduce the guard times and guard bands as shown in Fig. 4.9(b). CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

Q. 11 Give short notes on : Ethernet. Dec. 14

Ans. :

Both Internet and ATM were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other. For this the local area network (LAN) was introduced. The most popular LAN is called Ethernet.

The IEEE 802.3 standard is popularly called as Ethernet. It is a bus based broadcast network with decentralized control. It can operate at 10 Mbps or 100 Mbps or even above 1 Gbps. Computers on an Ethernet can transmit whenever they want to do so. If two or more machines transmit simultaneously, then their packets collide.

Then the transmitting computers just wait for an arbitrary time and retransmit their signal. There are various technologies available in the LAN market but the most popular one of them is **Ethernet.** Here we are going to see three generations of Ethernet :

1. Traditional Ethernet (10 Mbps)
2. Fast Ethernet (100 Mbps)
3. Gigabit Ethernet (1000 Mbps)

Traditional Ethernet was created in 1976 and has a data rate of 10 Mbps. The fast Ethernet is its next version and has a data rate of 100 Mbps.

The Gigabit Ethernet operates at the data rate of 1000 Mbps or 1 Gbps.

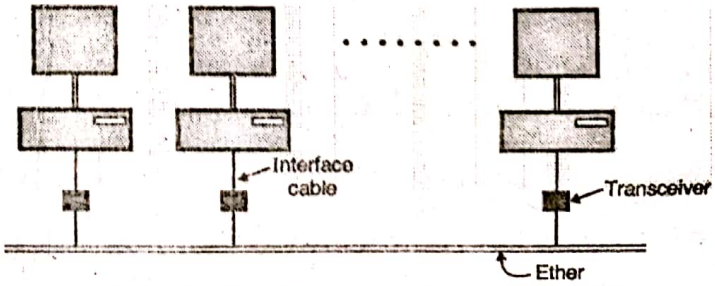
Why is it called Ethernet ?

This system is called as Ethernet after the luminiferous ether through which the electromagnetic radiation was once thought to propagate.

Transmission medium :

The transmission medium is thick co-axial cable (called ether) upto 2.5 km long. Repeaters are placed after every 500 meters. Upto 256 machines can be attached to the multidrop cable.

The architecture of the original Ethernet is shown in Fig. 4.10.



(G-293) **Fig. 4.10 : Architecture of original Ethernet**

Scanned by CamScanner

The original Ethernet was standardized as IEEE 802.3 standard. The committee also standardized a token bus (802.4) and token ring (802.5) standards which were not as popular as Ethernet.

Computer connected to Internet via LAN :

When a computer is connected to Internet via LAN, it has to use all the five layers of the internet model. The three upper layers (network, transport and application) are common to all the LANs.

The data link layer is divided into two sublayers namely the logical link control (LLC) and the medium access control sublayer (MAC). The LLC sublayer is designed to be the same for all the LANs so that all the LANs can be connected to each other and operate without any problem.

This means that only the MAC sublayer and physical layer of various LANs will be different from each other. If we compare different types of Ethernets then it is observed that, the MAC sublayer is slightly different but the physical sublayer is almost the same.

Q. 12 Make a comparative study of switched ethernet, fast ethernet and gigabit ethernet. Dec. 13

Ans. :

Switched Ethernet :

The concept of bridged LAN can be extended to the switched LAN. An N port switch is used to connect the N stations that are present in the given LAN.

The bandwidth is shared only between the stations and the switch. The collision domain is divided into N domains. The packet handling becomes faster due to the use to layer-2 switches.

Fast Ethernet :

Fast Ethernet is the protocol designed to work at higher data rates than the traditional one. Typically it can support the data rates upto 100 Mbps. The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

Autonegotiation :

This is the new feature of the fast Ethernet. The autonegotiation will make it possible to negotiate on the mode or data rare of operation between the communicating devices.

Gigabit Ethernet :

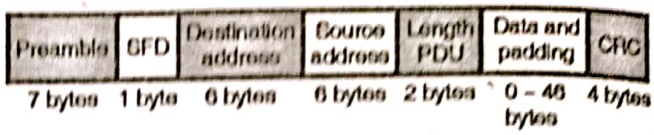
The gigabit Ethernet protocol has been designed in order to operate at data rates upto 1000 Mbps or 1 Gbps. This is the highest bit rate of all the types. The MAC layer was supposed to remain unchanged for all the versions of the Ethernet but it does not remain so when such a high data rate is to be supported.

The Gigabit Ethernet is capable of operating in either half duplex or full duplex modes.

Q. 13 Write short notes on : Ethernet frame formats. May 12

Ans. :

Fig. 4.11 shows the frame format of traditional Ethernet.



(G-305) **Fig. 4.11 : Traditional Ethernet frame**

Frame format :

The 64-bit (8 bytes) preamble allows the receiver to synchronize with the signal, it is a sequence of alternating 0's and 1's.

DA and SA :

Both the source and destination hosts are identified with a 48-bit (6 bytes) address. These are indicated by the byte number entered in the destination address (DA) and source address (SA) fields of the frame. The packet type field serves as the de-multiplexing key.

Data :

Each frame contains upto 1500 bytes of data. The minimum size of a frame is 46 bytes of data, the reason for this is that the frame must be long enough to detect a collision. Each frame includes 32 bit (4 bytes) checksum. CRC is the last field in the Ethernet frame. The Ethernet is a bit-oriented framing protocol. An Ethernet frame has 14-byte header, two 6-bytes addresses and 2-byte type field. The sending adapter attaches the preamble, CRC and postamble before transmitting and the receiving adapter removes them.

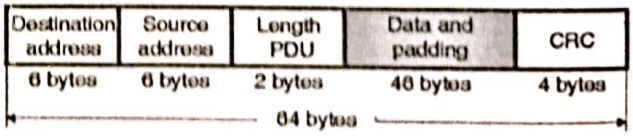
Start Frame Delimiter (SFD) :

This is the second field in the Ethernet frame and it is of 1 byte length. The byte stored at this field is 10101011. This field signals the beginning of the frame. The SDF is used to communicate to the station that this is the last chance for synchronization. The last two bits 11 alert the receiver that the next field in the frame contains the destination address.

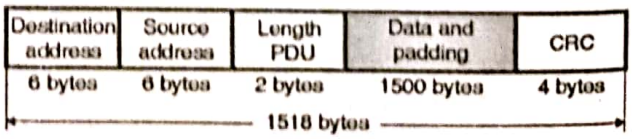
Q. 14 State the reasons for having a minimum length requirement for a frame in Ethernet. How is it achieved ? Dec. 13

Ans. :

There is a restriction imposed on the minimum and maximum length of the frame of the Ethernet. The minimum frame length is 512 bits or 64 bytes and the maximum frame length is 12,144 bits or 1518 bytes. The format of the minimum length frame is shown in Fig. 4.12(a) and that of the maximum length frame is shown in Fig. 4.12(b).



(a) Minimum length frame



(b) Maximum length frame

(G-306) **Fig. 4.12 : Minimum and Maximum length frame formats of traditional Ethernet**

Scanned by CamScanner

The restriction on the minimum length is to ensure correct operation of CSMA/CD, whereas the restriction on the maximum length is just out of some historical reasons.

Q. 15 1 Gbps CSMA/CD LAM is to be designed over 1 km cable without repeater. The cable supports signal speed of 200,000 km/sec. What is the minimum frame size that data link layer should consider. Dec. 03, Dec. 16

Ans. :

Propagation speed = 200000 km/sec.

Length of cable = 1 km

Propagation Time = $\frac{1}{200000} = 5 \times 10^{-6}$ s = 5 μ sec

Transmission speed = 1 Gbps.

Number of bits in cable :

Number of bits sender can transmit from time it sends 1st bit to the time that bit reaches end of cable.

$1 \times 10^9 \times \frac{1}{20000} = 0.5 \times 10^5 = 5 \times 10^4$ bits.

Frame size = $5 \times 10^4 \times 2$

= 10,000 bits

Total round time = 5 × 2 = 10 μ sec.

For collision detection frame should take at least 10 μS to send.

Data rate = 1000 bit per μS.

Thus 10,000 bits could be sent in 10 μS. Thus frame size should be at least 10,000 bits.

Q. 16 A pure ALOHA network transmits 200 bit frames on a shared channel of 200 kbps.

What is the throughput if the system (all stations together) produces ?

1. **1000 frames per second**
2. **500 frames per second**
3. **250 frames per second.** Dec. 16

Ans. :

Given : Rate of transmission = 200 kbps

= 200000 bps

Frame length = 200 bits

To find : Throughput

1. Number of frames / sec = 1000 frames / sec.

   The maximum throughput for a pure ALOHA system is 0.184

   ∴ Throughput = 1000 × 0.184

   = 184 frames /sec

2. Number of frames / sec = 500

   ∴ Throughput = 500 × 0.184

   = 92 frames / sec

3. Number of frames / sec = 250

   ∴ Throughput = 200 × 0.184

   = 36.8 frames / sec

Throughput of all stations = 184 + 92 + 36.8

= 312.8 frames / sec.

Q. 17 Explain the process of learning in case of transparent bridge. Dec. 09

Bridge learning :

When a frame arrives at one of the ports of a bridge, it has to make a decision about forwarding the frame to another port. This decision is made based on the destination address of the frame.

In order to make such decisions every bridge needs a table called **forwarding table or forwarding database.**

This table indicates which side of the port the destination station is attached to, directly or indirectly. The format of a forwarding table is shown in Table 4.1.

Table 4.1 : Format of a forwarding table

MAC address	Port

Note that in practice there are a few thousand entries in a forwarding table. Now see how to fill up these forwarding tables. It is filled up by a process called as "bridge learning".

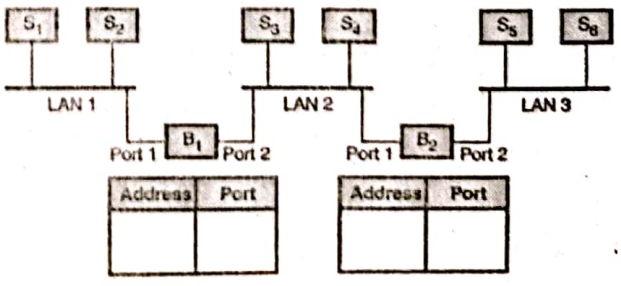
The basic bridge learning process is as follows :

Bridge learning procedure :

1. When a bridge receives a frame, it first compares the source address of the frame with each entry in the forwarding table. If no match is found, then the bridge will add this source address alongwith the port number on which the frame was received, to the forwarding table.
2. The bridge compares the destination address of the received frame with each entry in the forwarding table. If a match is found, then the bridge forwards the frame to the port indicated in the entry. But if this port is same as the one on which the frame was received, then the frame is discarded. Finally if a match is not found, then the bridge will send that frame on all its ports except the one on which the frame was received.

Example on bridge learning :

Consider the network shown in Fig. 4.13(a). Assume that forwarding tables of both the bridges are initially empty.



(L-649) **Fig. 4.13(a) : Example network**

Scanned by CamScanner

1. S_2 sends a frame to S_1 :

If S_2 sends a frame to S_1, then B_1 compares the source address of the received frame with the existing entries. So here S_2 is the sender and S_1 is destination. But there are no entries in B_1 table. So it adds the address of S_2 in its forwarding table as shown in Fig. 4.13(b). Then B_1 compares the destination address of the received frame with the existing entries. But the table is empty. So the bridge B_1 thinks of flooding the frames. But then it understands that the **destination S_1 is connected on the same port (Port 1) on which the frame has been received.** So B_1 will note down the address of S_1 in its table and **discard the frame.** This is because bridge B_1 is not required to be used when a communication between S_1 and S_2 is to be made. The traffic is now completely isolated in LAN 1, and the updated bridge tables are shown in Fig. 4.13(b).

B_1

Address	Port
S_2	1
S_1	1

B_2

Address	Port

Fig. 4.13(b) : Forwarding tables after $S_2 \rightarrow S_1$

2. S_5 transmits to S_4 :

The two stations correspond to two different LANs. S_5 is the sender and S_4 is the destination. First B_2 records the address of S_5 and port number (Port 2) because the address of S_5 is not found in its forwarding table. Then B_2 checks the destination address. Since there are no entries, it will add S_4 and port 1 in its table as shown in Fig. 4.13(c). Bridge B_2 will forward the frame to port 2 of B_1 as well as to LAN 2 where S_4 will receive it. When this frame arrives at port 2 of B_1 it also adds the source address i.e. S_5 and port 2 in its table as shown in Fig. 4.13(c). However the destination address (S_4) is on the same port (2) of B_1 on which it has received the frame. So it will note down S_4 and port 2 in its table but **discard** the frame.

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2

B_2

	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1

(G-1970) Fig. 4.13(c) : Forwarding tables after $S_5 \rightarrow S_4$

The table entries for the remaining transmissions are given in Figs. 4.13(d) and (e).

3. S_3 transmits to S_5 :

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2
$S_3 \rightarrow S_5$	S_3	2

B_2

	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1
$S_3 \rightarrow S_5$	S_3	2

(G-1971) Fig. 4.13(d) : Tables after $S_3 \rightarrow S_5$

4. S_1 transmits to S_2 :

No change in the tables.

5. S_6 transmits to S_5 :

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2
$S_3 \rightarrow S_5$	S_3	2

B_2

	Address	Port
$S_6 \rightarrow S_4$	S_6	2
	S_4	1
$S_3 \rightarrow S_5$	S_3	2
$S_6 \rightarrow S_5$	S_6	2

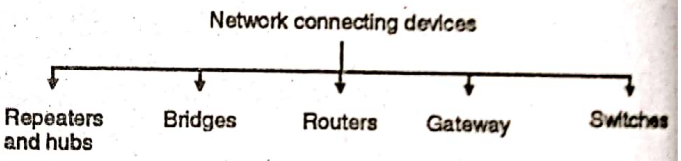
(G-1972) Fig. 4.13(e) : Table after $S_6 \rightarrow S_5$

Q. 18 Write short notes on : Internetworking devices.

Dec. 15

Ans. :

Different types of network connecting devices are as shown in Fig. 4.14.



(G-348) Fig. 4.14

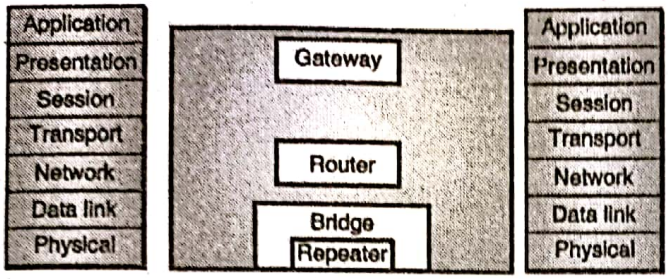
The relation between OSI reference model and various connecting devices is shown in Fig. 4.14(a).

Network connecting devices :

Two or more devices are connected to each other for the purpose of sharing data or resources from a network. A LAN may be spread over a larger distance than its media can handle effectively. The number of stations also can be more than a number which can be handled and managed properly. Such networks should be subdivided into smaller networks and these smaller subnetworks should be connected to each other through connecting devices. A device called a repeater is inserted into the network to increase the coverable distance or a device called a bridge can be inserted for traffic management. When two or more separate networks are connected for exchanging data or resources it creates an internetwork. Routers and gateways are used for internetworking. Each of these device type interacts with protocols at different layers of the OSI model. Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer. Bridges utilize addressing protocols and can affect the flow control of a single LAN. Bridges are most active at the data link layer. Routers provide links between two separate but same type LANs and are active at the network layer.

Finally gateways provide translation services between incompatible LANs or applications and are active in all of the layers. Connecting devices and the OSI model is shown in Fig. 4.14(a).

Scanned by CamScanner



(G-806(a)) **Fig. 4.14(a) : Connecting devices and OSI model**

Categories of connecting devices :

Fig. 4.14(a) shows the relationship between the connecting devices and various layers of the internet model.

Table 4.2 : Role of networking devices

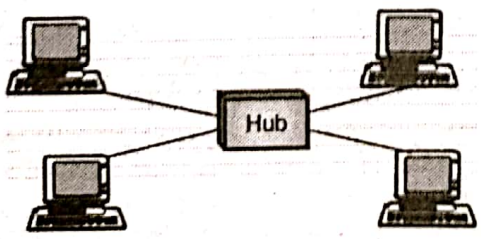
Sr. No.	Name of the device	Role
1.	Passive hub	Operate below the physical layer.
2.	Repeater	Regenerates the original signal. Operates in the physical layer.
3.	Bridge	Bridges utilize the address protocol. They can carry out the traffic management. They are most active in the data link layer.
4.	Routers	Routers provide connections between two separate but compatible networks. It works in the network layer.
5.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.

Q. 19 Explain with example : Hubs.

May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

Ans. : The general meaning of the word hub is any connecting device. But its specific meaning is multiport repeater. It is normally used for connecting stations in a physical star topology. All networks require a central location to connect various segments of media coming from various nodes. Such a central location is called as a hub. A hub organizes the cables and relays signals to the other media segments as shown in Fig. 4.15. There are three main types of hubs :

1. Passive hubs 2. Active hubs 3. Intelligent hubs



(G-350) **Fig. 4.15 : Hub**

Passive Hubs :

A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.

A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal. With a passive hub, each computer receives the signals sent from all the other computers connected to the hub. This type of hub is a part of communication media. Hence its location is below the physical layer.

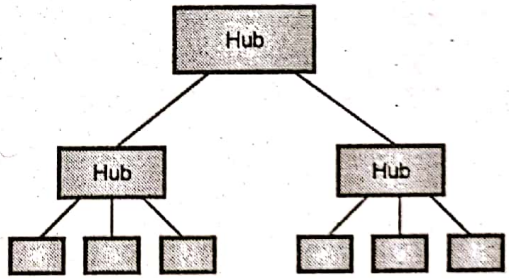
Active Hubs :

They are like passive hubs but have electronic components for regeneration and amplification of signals. By using active hubs the distance between devices can be increased. An active hub is equivalent to a multipoint repeater. The main drawback of active hubs is that they amplify noise as well along with the signals. They are more expensive than passive hubs as well.

Intelligent Hubs :

In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection. A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.

Hubs can also be used to create multiple levels of hierarchy as shown in Fig. 4.15(a).



(L-646) **Fig. 4.15(a) : Hubs to create multiple levels of hierarchy**

Q. 20 Explain with example : Repeater.

Dec. 09, May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

Ans. :

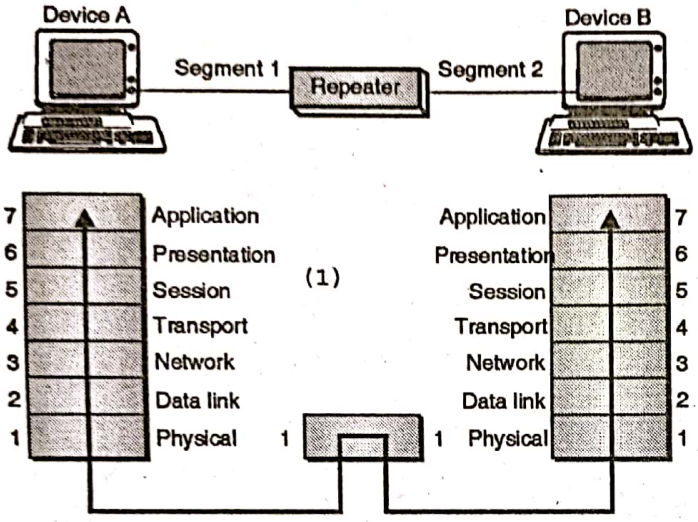
A repeater is a connecting device which can operate only in the physical layer. All transmission media weaken the electromagnetic waves that travel through them. Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are called repeaters. A repeater receives a signal and before it gets attenuated or corrupted, regenerates the original signal. Thus we can use a repeater to extend the physical length of LAN as shown in Fig. 4.15(a).

Repeater is not an amplifier because amplifiers simply amplify the entire incoming signal along with noise.

Scanned by CamScanner

Signal – regenerating repeaters create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it and retransmitting only the desired information. The original signal is duplicated, boosted to its original strength and sent as shown in Figs. 4.15(a) and (b).

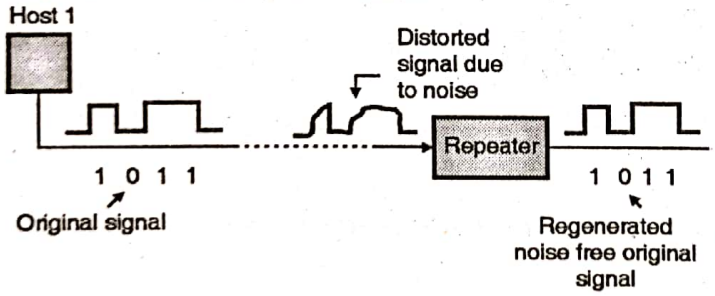
A repeater does not connect two LANs. It connects only two devices connected in the same LAN.



(G-351) **Fig. 4.15(a) : Repeater in OSI model**

It cannot connect two LANs of a different protocols. A repeater forwards every frame, it cannot filter out some frames and let the others pass through. A repeater should be placed at a precise point on the link. Such that the signal reaches it before the noise has induced an error in any of the transmitted bits. Fig. 4.15(b) illustrates the function of a repeater.

Repeaters operate at the physical layer of the OSI model and they deal with the actual physical signals.



(G-352) **Fig. 4.15(b) : Function of a repeater**

Q. 21 Explain with example : Bridges.

Dec. 09, May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

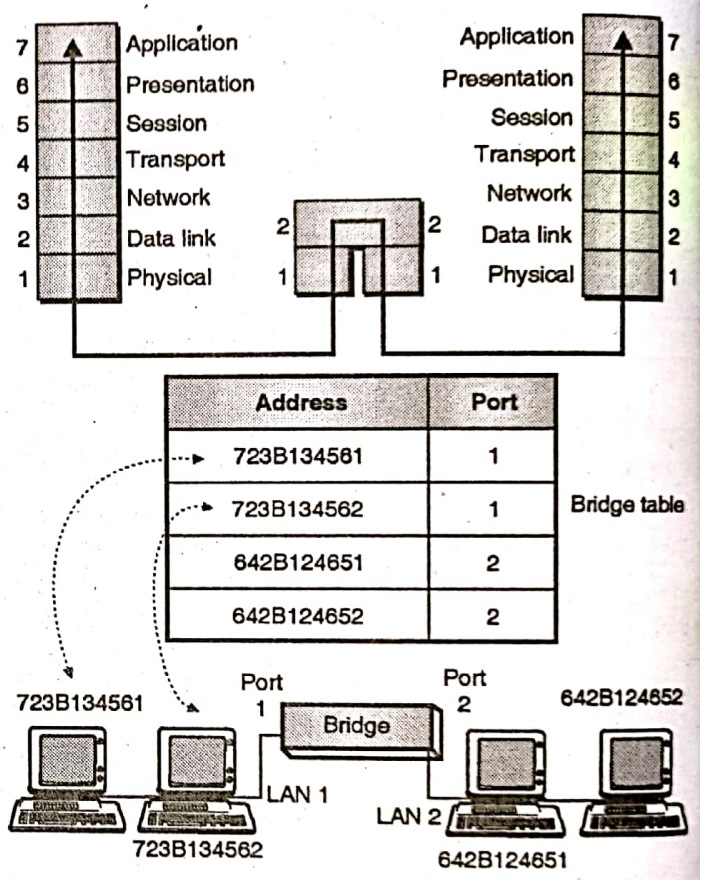
Ans. :

A bridge can operate in the physical layer as well as in the data link layer of the OSI model. It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.

Filtering :

The major difference between the bridge and repeater is that the bridge has a filtering capability. That means a bridge will check the destination address of a frame and make a decision about whether the frame should be forwarded or dropped. If the frame is to be forwarded, then the bridge should specify the port over which it should be forwarded. In order to achieve this a bridge has a table relating the addresses and ports as shown in Fig. 4.16. If a frame for 723B134561 arrives at port 2 then the bridge goes through its table and understands that the frame is to be sent out on port 1 so it will do so.

In Fig. 4.16 a two port bridge is shown but in reality a bridge has more than two ports.



(G-354) **Fig. 4.16 : Bridge and bridge table**

It is important to note that the bridges do not change the physical address contained in the frame.

Types of bridges :

The bridges are of two types :

1. Transparent bridges and 2. Routing bridges.

Transparent bridge is a bridge in which the stations are not at all aware of the existence of the bridge. Transparent bridges keep a table of addresses in memory to determine where to send data. The duties of a transparent bridge are as follows :

1. Filtering frames 2. Forwarding and 3. Blocking.

In source routing a sending station defines the bridges that should be visited by the frames. The addresses of these bridges are included in the frame. So a frame contains not only the source and destination address but also the bridge addresses. Source routing bridges are used to avoid a problem called looping. These bridges were designed for the token ring LANs. But these LANs are not very common now a days.

Scanned by CamScanner

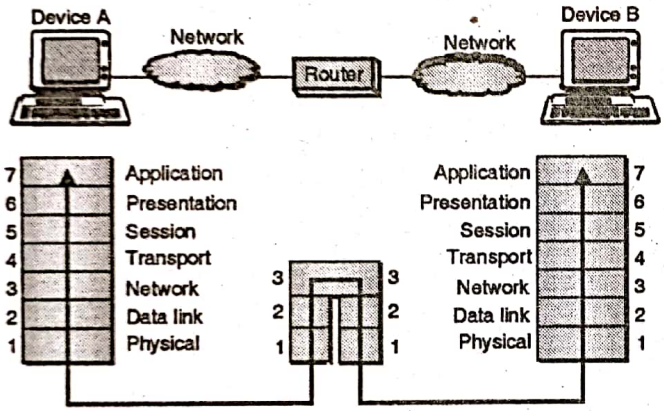
Q. 22 Explain with example : Router.

May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13

Ans. :

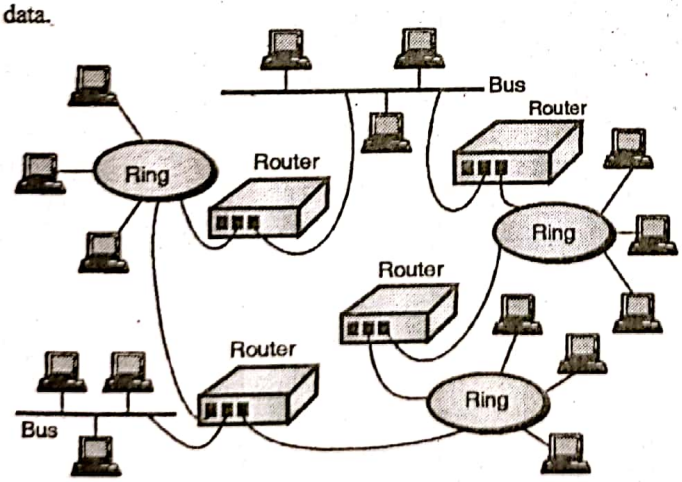
Routers are devices that connect two or more networks as shown in Figs. 4.17(a) and (b). They consist of a combination of hardware and software. The hardware can be in the form of a network server, a separate computer or a special device, as well as the physical interfaces to the various networks in the internetwork. Various types of networks can be interconnected through routers as shown in Fig. 4.17(b). The software in a router are the operating system and the routing protocol. Management software can also be used.

Routers use logical and physical addressing to connect two or more logically separate networks. The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.



(G-364) **Fig. 4.17(a) : A router in the OSI model**

Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.



(G-365) **Fig. 4.17(b) : Routers in an internet**

Data is grouped into packets, or blocks of data. Each packet has a * information. The two methods of route discovery are :

1. Distance vector routing 2. Link state routing.

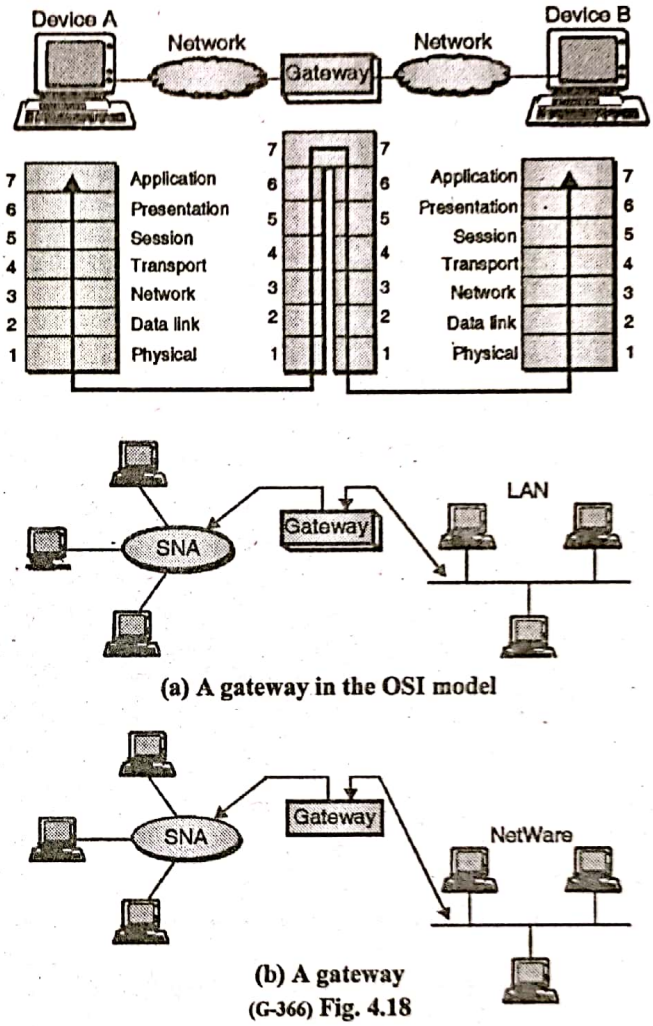
Note :

1. Routers work at the network layer of the OSI model.
2. With static route selection, packets always follow a pre-determined path.

Q. 23 Explain Gateways.

May 10, May 11, Dec. 11, May 12, Dec. 13

Ans. :



(a) A gateway in the OSI model

(b) A gateway

(G-366) **Fig. 4.18**

When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a gateway is used. A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks as shown in Figs. 4.18(a) and (b). Gateways comprise of software, dedicated hardware or a combination of both. Gateway operate through all the seven layers of the OSI model and all five layers of the internet model. A gateway can actually convert data so that it works with an application on a computer on the other side of the gateway. For e.g. a gateway can receive e-mail message in one format and convert them into another format.

Gateways can connect systems with different communication protocols, languages and architecture. For e.g. IBM networks using Systems Network Architecture (SNA) can be connected to LANs using a gateway.

Gateways are slow because they need to perform intensive conversions.

Scanned by CamScanner

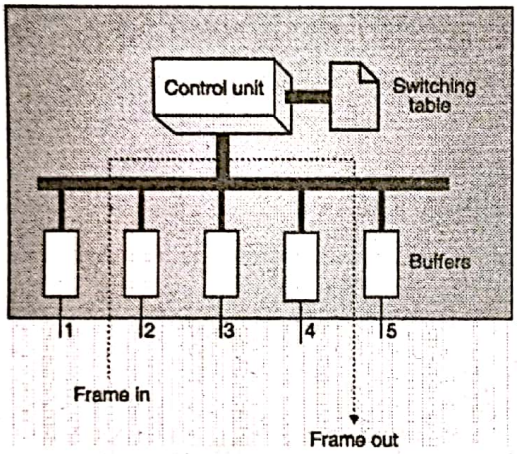
Q. 24 Explain Switches.

May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13

Ans. : A switch is a device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in a LAN. The switch has a buffer for each link to which it is connected. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If the outgoing link is free, the switch sends the frame to that particular link. Switches are of two types :

1. Store - and - forward switch 2. Cut - through switch.

A store - and - forward switch stores the frame in the input buffer until the whole packet has arrived. A cut-through switch, forwards the packet to the output buffer as soon as the destination address is received.



(G-367) **Fig. 4.19 : Switch**

Concept of a switch is shown in Fig. 4.19. As shown in the Fig. 4.19 a frame arrives at port 2 and is stored in the buffer. The CPU and the control unit, using the information in the frame consult the switching table to find the output port. The frame is then sent to port 5 for transmission.

Note : Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

Q. 25 Differentiate between Hub and Switch.

Dec. 09, Dec. 10

Ans. :

Sr. No.	Hub	Switch
1.	It is a broadcast device.	It is a point to point device.
2.	It operates at physical layer.	It operates at datalink layer.
3.	It is not an intelligent device.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5.	It cannot be used as a repeater.	It can be used as a repeater.
6.	Not a sophisticated device.	It is a sophisticated device.
7.	Not very costly.	Costly.

Chapter 5 : Network Layer

Q. 1 Differentiate between virtual-circuit and datagram subnets.

Dec. 09, May 10, May 11, May 12

Ans. :

Table 5.1

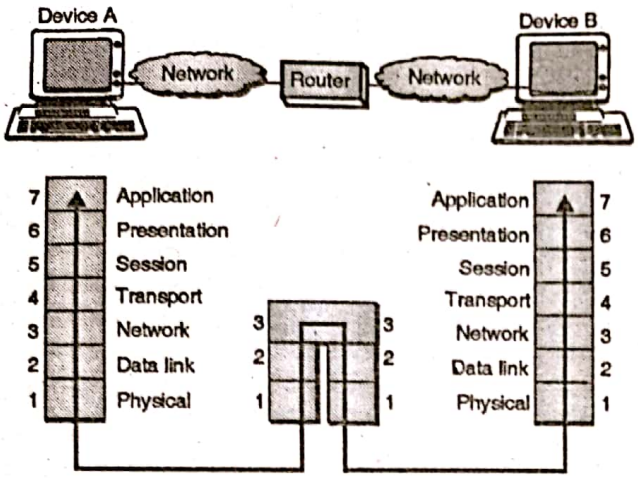
Sr. No.	Parameter	VC subnet	Datagram subnet
1.	Connection set up	Required	Not required.
2.	Addressing	Each packet contains a short VC number	Each packet contains the source as well as destination address.
3.	Repairs	Harder to repair	Easy to repair.
4.	State information	A table is needed to hold the state information.	Subnet does not hold state information.
5.	Routing	Route chosen is fixed. All packets follow this route. This is static routing.	Each packet is routed independently. This is dynamic routing.
6.	Congestion control	Easy	Difficult.
7.	Effect of router failure.	All VCs which passed through failed router are terminated.	No other effect except for the packets lost at the time of crash.

Q. 2 What does routing mean and how does it works ? Describe routing table structure.

May 04

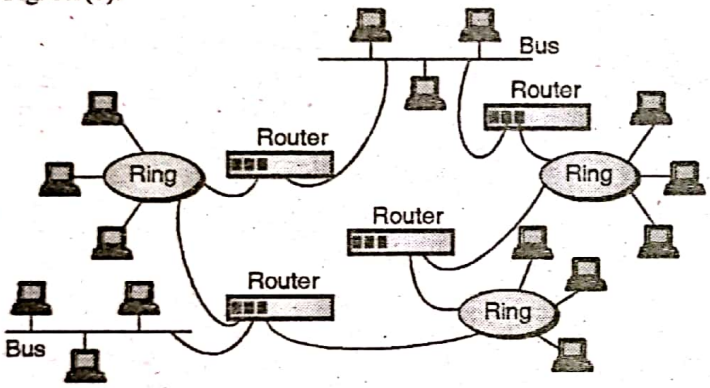
Ans. : Routers are devices that connect two or more networks as shown in Figs. 5.1(a) and (b). They consist of a combination of hardware and software.

Scanned by CamScanner



(G-446) **Fig. 5.1(a) : A router in the OSI model**

The hardware can be in the form of a network server, a separate computer or a special device as well as the physical interfaces to the various networks in the internetwork. Various types of network can be interconnected through routers as shown in Fig. 5.1(b).



(G-447) **Fig. 5.1(b) : Routers in an internet**

The software in a router are the operating system and the routing protocol. Management software can also be used. Routers use logical and physical addressing to connect two or more logically separate networks. The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.

Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data. Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address. The network address allows routers to calculate the optimal path to a workstation or computer.

Route discovery is the process of finding the possible routes through the internetwork and then building routing tables to store that information. The two methods of route discovery are :

1. Distance vector routing
2. Link state routing.

Note : Routers work at the network layer of the OSI model. With static route selection, packets always follow a pre-determined path.

Routing Tables :

The routing table for a host or a router consists of an entry for each destination, or a combination of destinations to route the IP packets. Routing tables can be of two types :

1. Static routing tables 2. Dynamic routing tables

1. Static routing table :

The information in the static routing tables is entered manual. The route of a packet to each destination is entered into the table by the administrator. This routing table cannot update itself automatically. It has to be changed manually as and when required.

Hence static routing table is useful only for small networks.

2. Dynamic routing table :

The dynamic routing tables can get automatically updated by using a dynamic routing protocol such as RIP, OSPF or BGB. The structure of a dynamic routing table is shown in Table 5.2.

Table 5.2 : Format of dynamic routing table

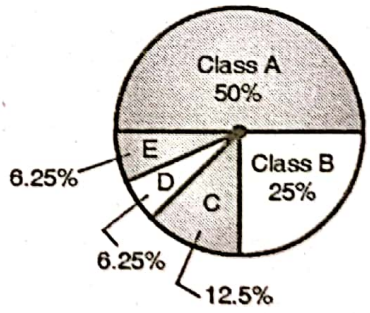
Mask	Network Address	Next hop address	Interface	Flags	Reference count	Use

Q. 3 Describe the classification of IP-addresses in IPv4.

Dec. 05, Dec. 06, Dec. 07, May 08, May 09, May 10, May 17

Ans. :

In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E. Fig. 5.2 shows the percentage of occupation of the address space by each class. The number of class A addresses is the highest i.e. 50% and those of classes D and E is the lowest i.e. 6.25%.



Class	No. of addresses	
A	2^{31}	50%
B	2^{30}	25%
C	2^{29}	12.5%
D	2^{28}	6.25%
E	2^{28}	6.25%

(G-2003) **Fig. 5.2 : Classful addressing occupation of address space**

Scanned by CamScanner

Formats of Various Classes :

(G-531) **Fig. 5.2(a) : Class A IPv4 address formats**

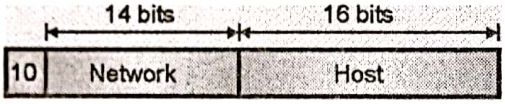
Class A format :

The formats used for IPv4 address are as shown in Fig. 5.2. The IPv4 address for class A networks is shown in Fig. 5.2(a). The network field is 7 bit long as shown in Fig. 5.2(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 126. But the host numbers will range from 0.0.0.0 to 127.255.255.255. Thus in class A, there can be 126 types of networks and 17 million hosts.

The "0" in the first field identifies that it is a class A network address.

Class B format :

The class B address format is shown in Fig. 5.2(b). The first two fields identify the network, and the number in the first field must be in the range 128 - 191.



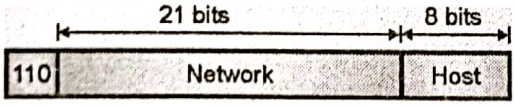
(G-532) **Fig. 5.2(b) : Class B format**

Class B networks are large. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65,534 (216-2) hosts in a class B network. Most of the 16,382 class B addresses have been allocated. The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

Example : 128.89.0.26, for host 0.26 on net 128.89.

Class C format :

The class C address format is shown in Fig. 5.2(c).



(G-533) **Fig. 5.2(c) : Class C format**

The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

The class D address format is shown in Fig. 5.2(d).

Fig. 5.2(d) : Class D format

The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

Fig. 5.2(e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

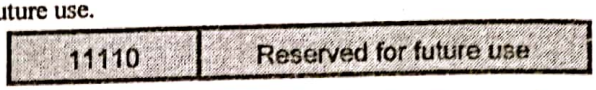


Fig. 5.2(e) : IPv4 address for class E network

The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255. So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

Q. 4 Explain masking. Dec. 06

Ans. :

When a packet arrives at the input of the router in the Internet, it uses an algorithm to extract the **network address** from the destination address in the received packet. This can be achieved by using a **network mask.**

Definition of default mask :

A **network mask** or **default mask** in classful addressing is defined as a 32-bit number obtained by setting all the "n" leftmost bits to 1s and all the (32 – n) rightmost bits to 0.

Q. 5 Explain subnetting.

Dec. 06, May 07, May 08, Dec. 08, May 16

Ans. :

The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host. But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :

1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

Definition of subnetting :

We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses. In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets.**

Each such subnet has its own **subnet address.**

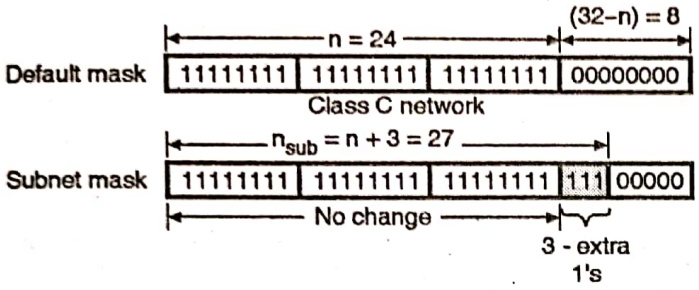
Subnet mask :

The **network mask** or **default** mask is used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting** is **not** to be done.

Scanned by CamScanner

But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet. Fig. 5.3 shows the format of a subnet mask. Each subnet has its own **net id** and **host id.**

If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 5.3. In Fig. 5.3, we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.

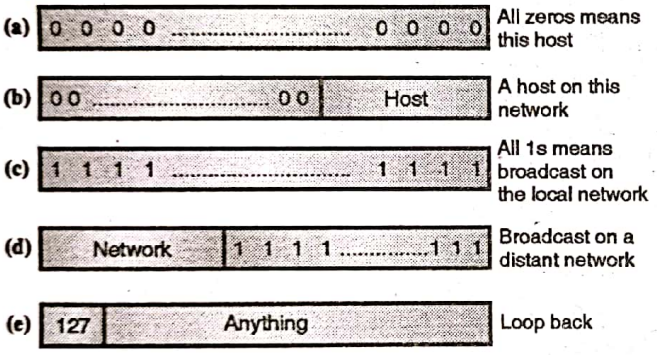


(G-2011) **Fig. 5.3 : Default and subnet masks**

Q. 6 Discuss various special IP addresses. May 09

Ans. :

Fig. 5.4 shows some special IP addresses.



(G-540) **Fig. 5.4 : Special IP addresses**

All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network. The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward. The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 5.4(b). The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 5.4(c). Refer Fig. 5.4(d). This is an address with proper network number and all 1s in the host field. This address allow machines to send broadcast packets to distant LANs anywhere in the Internet. If the address is "127. Anything" as shown in Fig. 5.4(e) then it is a reserved address **loopback testing.** This feature is also used for debugging network software.

Q. 7 A network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle ? Dec. 04

Ans. : The maximum number of hosts a network handle can be almost 254 (28-2) host.

Q. 8 A class A network on the internet has a subnet mask of 255.255.224.0. What is the maximum number of hosts per subnet ? May 05

Ans. :

A subnet mask of 255.255.224.0 corresponds to the following pattern.

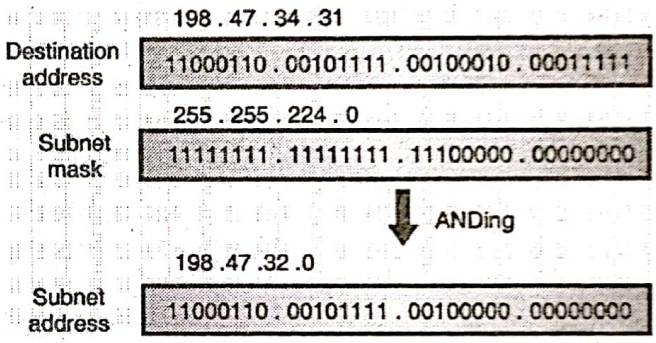
255	255	244	0
11111111	11111111	111	00000	00000000

Due to 3 additional 1s (shaded portion) there will be $2^3 = 8$ subnets and the number of hosts per subnet will be $2^{13} = 8192$.

Q. 9 What is subnet address if the destination address is 198.47.34.31 and subnet mask is 255.255.224.0 Dec. 09

Ans. :

To find subnet address we have to AND the IP address and the subnet mark as shown Fig. 5.5.



(G-804) **Fig. 5.5**

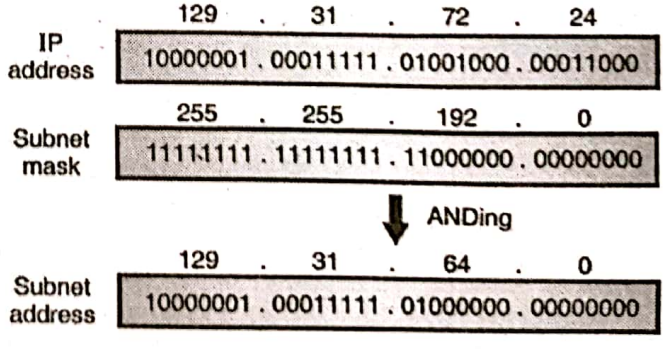
Thus the required subnet address is 198.47.32.0

Q. 10 What is subnetting ? What are the default subnet masks ? Find the subnet address if the IP address is 129.31.72.24 and subnet mask is 255.255.192.0. Dec. 15

Ans. :

Please refer Q.5 for subnetting.

To find the subnet address we have to AND the IP address and the subnet mask as shown in Fig. 5.6.



(G-1868) **Fig. 5.6**

Thus the required subnet address is 129.31.64.0.

Scanned by CamScanner

Q. 11 What is subnetting ? Given the class C network 192.168.10.0 use the subnet mask 255.255.255.192 to create subnets and answer the following :

1. **What is the number of subnets created ?**
2. **How many hosts per subnet ?**
3. **Calculate the IP address of the first host, the last host and the broadcast address of each subnet.** May 17

Ans. :

For subnetting refer Q.5.

Given : IP address : 192.168.10.0 (class C)
Subnet mask : 255.255.255.192

Step 1 : Number of subnets and number of hosts :

255.255.255.192 ...(Given)

11111111 · 11111111 · 11111111 · 11000000

The number of subnets are determined by the number of extra 1's.

$\therefore$ Number of extra 1's = 2

$\therefore$ Number of subnets = $2^2 = 4$ ...Ans.

The value of n is 26 which means the number of hosts per subnet is,

$2^{32-26} = 2^6 = 64$ ...Ans.

Step 2 : IP address of the first host, last host and broadcast address :

The following is the range of subnets :

Subnet	Subnet range
1	192.168.10.0 to 192.168.10.63
2.	192.168.10.64 to 192.168.10.127
3.	192.168.10.128 to 192.168.10.191
4.	192.168.10.192 to 192.168.10.255

IP address of first host : 193.129.65.1

IP address of last host : 254.190.126.62

Broadcast address : 255.191.127.63

Q. 12 A router has following CIDR entries in its routing table :

Address/Mask	Next Hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives ?

1. **135.46.63.10** 2. **192.53.56.7**

Dec. 10, Dec. 11, May 16

Ans. :

CIDR – Classless Inter Domain Routing :

IP is being heavily used for decades. However, due to the exponential growth of internet, IP is running out of addresses. This is a potential disaster. One of the solutions is CIDR (Classless Inter Domain Routing). The CIDR is based on the principle of allocating the remaining IP addresses in variable-sized blocks regardless of the class. If a site needs say 2000 addresses, then a block of 2048 addresses on the 2048 byte boundary is given to it.

However the classless routing makes forwarding of packets more complicated.

Forwarding algorithm in the old classful system :

The steps followed in the old classful system for forwarding packets is as follows :

1. As soon as a packet arrives at a router, a copy of the IP address was shifted right by 28 bits to obtain a 4 bit class number.
2. A 16-way branch then sorts packets into class A, B, C and D (if supported) with eight of the cases for class A, four of the cases for class B, two of the cases for class C and one each for D and E.
3. The code for each class then masked off the 8–, 16–, or 24– bit network number and right aligned it in a 32 bit word.
4. The network number was then searched in the A, B or C table.
5. As soon as the entry was found, the outgoing line was decided and the packet was forwarded upon it.

Forwarding with CIDR :

The simple forwarding algorithm does not work with CIDR. Instead now each router table entry is extended by giving if a 32 bit mask. So now there is a single routing table for all networks (no different tables for class A, B, C, etc.) which consists of an array of triples. Each triple consists of an **IP address, subnet mask** and **outgoing line.** When a packet arrives at the input, the router first extracts its destination IP address. Then the routing table is scanned entry by entry to look for a match. It is possible that different entries with different subnet mask lengths match. In such a case the longest mask is used. For example if there is a match for a/20 mask and a/24 mask then /24 entry is used.

Solution of problem :

Convert the IP address to bits and then AND it with the subnet mask of the interface whose address is closest to that of the IP addresses. The result of the ANDing will give you the network address and the interface to send the packet to.

1. **IP = 135.46.63.10 :**

The interface whose address is closest to this IP is interface 1. This interface uses a 22 bit mask. So AND the given IP address with a 22 bit mask as follows :

Scanned by CamScanner

IP = 135.46.63.10 = 10000111.00101110.00111111.00001010
22 bit mask = 255.255.252.0 = 11111111.11111111.11111100.00000000
IP AND Mask = 10000111.00101110.00111100.00000000
∴ IP AND Mask = 135.46.60.0

(G-1973)

This result of ANDing matches with the network address of interface 1. Hence the router will forward this packet to interface 1.

2. **IP = 192.53.56.7 :**

The interface whose address is closest to this IP is interface 2. This interface uses a 23 bit mask. So AND the packet IP address with a 23 bit mask as follows :

IP = 192.53.56.7 = 11000000.00110101.00111000.00000111
23 bit mask = 255.255.254.0 = 11111111.11111111.11111110.00000000
IP AND Mask = 11000000.00110101.00111000.00000000
= 192.53.56.0

(G-1974)

This result of ANDing does not match with the network addresses of interface 0 or 1. Hence the packet will forwarded to the default i.e. Router 2.

Q. 13 What is the function of IP protocol ?

May 15, May 16, Dec. 17

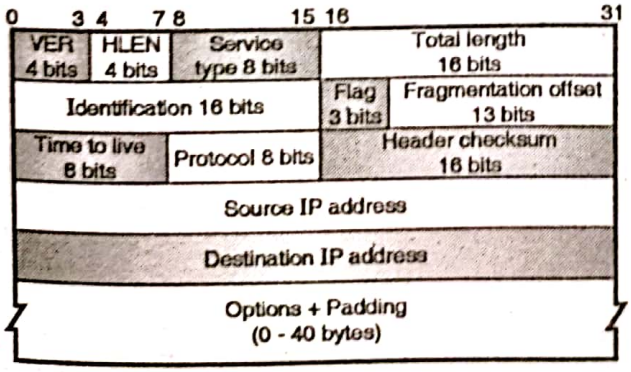
Ans. :

IP takes help from ARP in order to find the MAC (physical) address of the next hop. IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error. IP is basically designed for unicast delivery. But some new Internet applications as well as multimedia need multicast delivery. So for multicasting, IP has to use the services of another protocol called IGMP. IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

Q. 14 Describe the IPv4 header format in detail.

May 10, May 11, Dec. 11, May 12, May 13, Dec. 13, May 15, May 16, Dec. 17

Ans. : The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure is as shown in Fig. 5.7.



(G-2082) **Fig. 5.7 : IPv4 header format**

Various fields in the header format are as follows :

1. VER (Version) :

This is a 4 bit field which is used to define the version of IP protocol. The current version of IP is 4 i.e. IPv4 but in future it may be completely replaced by the latest version of IP i.e. IPv6. This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version. If the processing machine is using some other version of IP, then the datagram will be discarded.

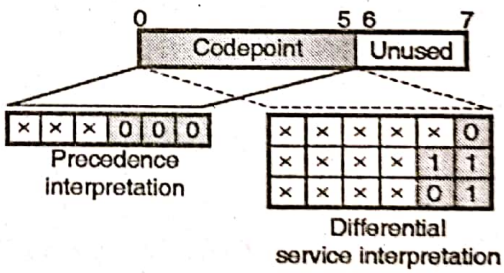
2. HLEN (Header length) :

This 4-bit long field is used for defining the length of the datagram header in 4-byte words. The value of this field is multiplied by 4 to get the length of the IPv4 header which varies between 20 and 60 bytes. When there are no options, the value of this field is 5 and the **header length** is 5 × 4 = 20 bytes.

When the value of option field is maximum the value of HLEN field is 15 and the corresponding header length is maximum i.e. 15 × 4 = 60 bytes.

3. Service type :

In the IPV4 designs of IP header, this field was called as **Type of Service (TOS)** field and its job was to define how the datagram should be handled. At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc. But now the interpretation of this field has been changed by IETF. This field is now supposed to define a set of **differential services.** Fig. 5.7(a) illustrates the new interpretation of the **service type** field.



(G-2083) **Fig. 5.7(a) : New interpretation of service type field**

As seen in Fig. 5.7(a), in the new interpretation, the service type field is divided into two subfields namely, the 6 bit **codepoint** subfield and a 2 bit **unused** subfield. We can use the 6-bit **codepoint** subfield in two different ways, as follows :

1. For the purpose of precedence interpretation.
2. For the differential service interpretation.

Precedence interpretation :

If the three right most bits are zeros, then the three leftmost bits are interpreted the same as the precedence bits in the service field (old interpretation). That means it is compatible with the old interpretation of this field. The precedence interpretation is used for defining the priority level of this datagram (from 0 to 7) in the situations like congestion.

Scanned by CamScanner

In the event of congestion, the datagrams with lowest precedence (0) will be discarded first.

Differential service interpretation :

When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation. In that case these 6 bits can be used for defining a total of 56 (64 – 8) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 5.2.

Table 5.2 : Values of codepoints

Category	Codepoint	Assigning authority
1.	× × × × × 0	Internet
2.	× × × × 1 1	Local
3.	× × × × 0 1	Temporary or Experimental

The first, second and third categories contain 24, 16 and 16 service types respectively. The Internet authorities assign the first category. The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

This 16 bit field is used to define the total length of the IP datagram. The total length includes the length of header as well as the data field. The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1) = 65535$ bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers. This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.

All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments. The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram. We can find the length of data by subtracting the header length from the total length. The header length can be obtained by multiplying the contents of HLEN field by four.

$\therefore$ Length of data = Total length – header length

The total length (maximum value) of 65,535 bytes might seem to be large but in future the size of IP datagram is likely to increase further because the improvement in technology will allow more bandwidth.

Why do we need the total length field ?

We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame. Then why to include this field ?

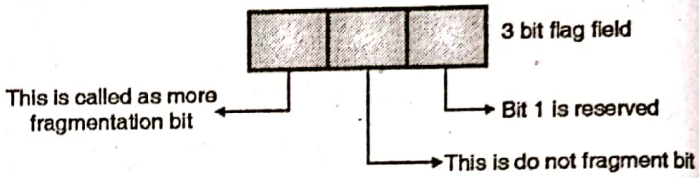
The answer to this question is that in many situations we do not need this field at all. But in some special situations, only the datagram is not encapsulated in the frame but there are some padding bits as well that are included. In such situations, the machine (host or router) that decapsulates the datagram, needs to check the **total length** field so as to understand how much is the data and how much is the padding ?

5. Identification :

This field is used to identify the datagram originating from the source host. When a datagram is fragmented, the contents of the identification field get copied into all fragments. This identification number is used by the destination to reassemble the fragments of the datagram.

6. Flags :

Flags : This is a three bit field. The 3 bits are as shown in Fig. 5.7(b).



(G-527)**Fig. 5.7(b) : Flag bits**

First bit is reserved, and it should be 0. The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented. But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.

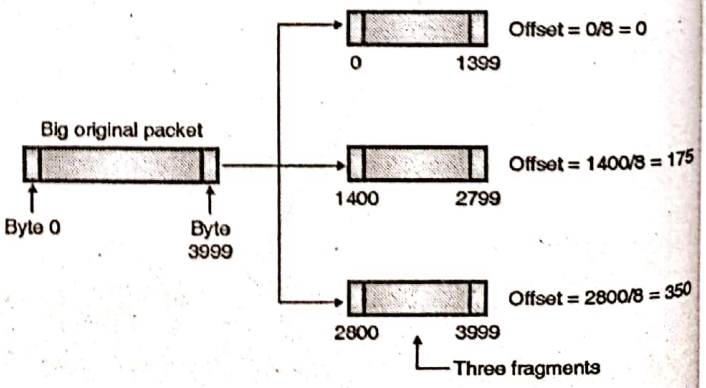
The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. Fragmentation offset :

This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram. It is the offset of the data in the original datagram measured in units of 8 bytes.

To understand this refer Fig. 5.7(c).

The original IP packet (datagram) contains 4000 bytes numbered from 0 to 3999. It is fragmented into three fragments. The first fragment contains 1400 bytes numbered from 0 to 1399. The offset for this fragment is 0/8 = 0. Similarly the offsets for the other two fragments are 1400/8 = 175 and 2800/8 = 350 respectively as shown in Fig. 5.7(c). The offset is measured in units of 8 bytes. Because the length of the offset field is 13 bits, so the fragments should be of size such that first byte number is divisible by 8.



(G-528)**Fig. 5.7(c) : Example of fragmentation**

Scanned by CamScanner

8. Time to Live (TTL) :

This is an 8-bit field which controls the maximum number of routers visited by the datagram during its lifetime. A datagram has a limited lifetime for travelling through an Internet.

Originally the TTL field was designed to hold the **timestamp.** This timestamp value was decremented by one, everytime the datagram visits a router.

As soon as the timestamp value reduces to zero the datagram is discarded. But for this scheme to become successful, all the machines must have synchronized clocks and they must know the time taken by a datagram to travel from one router to the other. Today the TTL field is used to **control** the maximum number of hops i.e. router by a datagram. At the time of sending a datagram, the source host will store a number in the TTL field. This number is approximately twice the maximum number of routers present between any two hosts. Everytime this datagram visits a router, this value is decremented by one. If after decrementing, the value of TTL field reduces to zero then that router discards the datagram.

Need of TTL field :

Sometimes the routing tables in the Internet get corrupted, due to which a datagram may travel between two or more routers for a very long time but never ever gets delivered to the destination host. The TTL field is needed in such situations for **limiting the lifetime of a datagram.** The TTL field is also used to **limit the journey of a packet intentionally.** For example if a packet is to be confined to a local network only then a 1 is stored in the TTL field of this packet. As soon as it reaches the first router, then TTL field value is decremented from 1 to 0 and the packet will be discarded.

9. Protocol :

This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer. The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.

The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered. At the destination, the value of this field helps in the process of demultiplexing.

Table 5.3 shows some of the values of this field corresponding to different high level protocols.

Table 5.3

Value	Protocol	Value	Protocol
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

10. Header checksum :

A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

11. Source address :

This field is used for defining the IP address of the source. It is a 32 bit field.

12. Destination address :

This field is used for defining the IP address of the destination. It is also a 32 bit field.

13. Options :

Options are not required for every datagram. They are used for network testing and debugging.

Q. 15 State different types of routing algorithm.

Dec. 04, May 05, May 07, May 08, Dec. 08, Dec. 09, Dec. 12, May 13, Dec. 15

Ans. :

Routing algorithms can be divided into two groups :

1. Non-adaptive algorithms. 2. Adaptive algorithms.

1. Non-adaptive algorithms :

For this type of algorithms, the routing decision is not based on the measurement or estimation of current traffic and topology. However the choice of the route is done in advance, off-line and it is downloaded to the routers.

This is called as static routing.

2. Adaptive algorithms :

For these algorithms the routing decision can be changed if there are any changes in topology or traffic etc. This is called as dynamic routing.

Q. 16 Explain shortest path routing in detail. Dec. 05

Ans. :

This algorithm is based on the simplest and most widely used principle. Here a graph of subnet is prepared in which each node represents either a host or a router and each arc represents a communication link. So as to choose a path between any two routers, this algorithm simply finds the shortest path between them.

How to decide the shortest path ?

One way of measuring the path length is the number of hops. Another way (metric) is the geographical distance in kilometres. Some other metrics are also possible. For example we can label each arc (link) with the mean queuing and transmission delay and obtain the shortest path as the fastest path.

Labels on the arcs :

The labels on the arcs can be computed as a function of distance bandwidth, average traffic, mean queue length, cost of communication, measured delay etc. The algorithm compares various parameters and calculates the shortest path, on the basis of any one or combination of criterions stated above.

Various shortest path algorithms :

There are many algorithms for computing the shortest path between two nodes.

Scanned by CamScanner

Q. 17 One of them is Dijkstra algorithm. The other one is Bellman-Ford algorithm. Explain Dijkstra's algorithm as shortest path routing with example. May 10, Dec. 11

Ans. :

Dijkstra's algorithm is used for computing the shortest path from the root node to every other node in the network. The root node is defined as the node corresponding to the router where the algorithm is being run. The total number of nodes are divided into two groups namely the P group and T group. In the P group we have those nodes for which the shortest path has already been found.

In T group the remaining nodes are placed. The path to every node in the T group should be computed from a node which is already present in group P. We should find out every possible way to reach an outside node by a one hop path from a node which is already present in P and choose the shortest of these paths as the path to the desired node. We define two sets P (permanent) and T (temporary) of the nodes. In set P we have nodes to which the shortest path has already been found and in set T we have nodes to which we are considering the shortest paths. At the time of starting, P is initialized to the current node and T is initialized to null.

The algorithm then repeats the following steps :

1. Start from the desired node say p. Write p in the P set.
2. For this node p, add each of its neighbours n to T set.

The addition of these nodes in T will have to satisfy the following conditions :

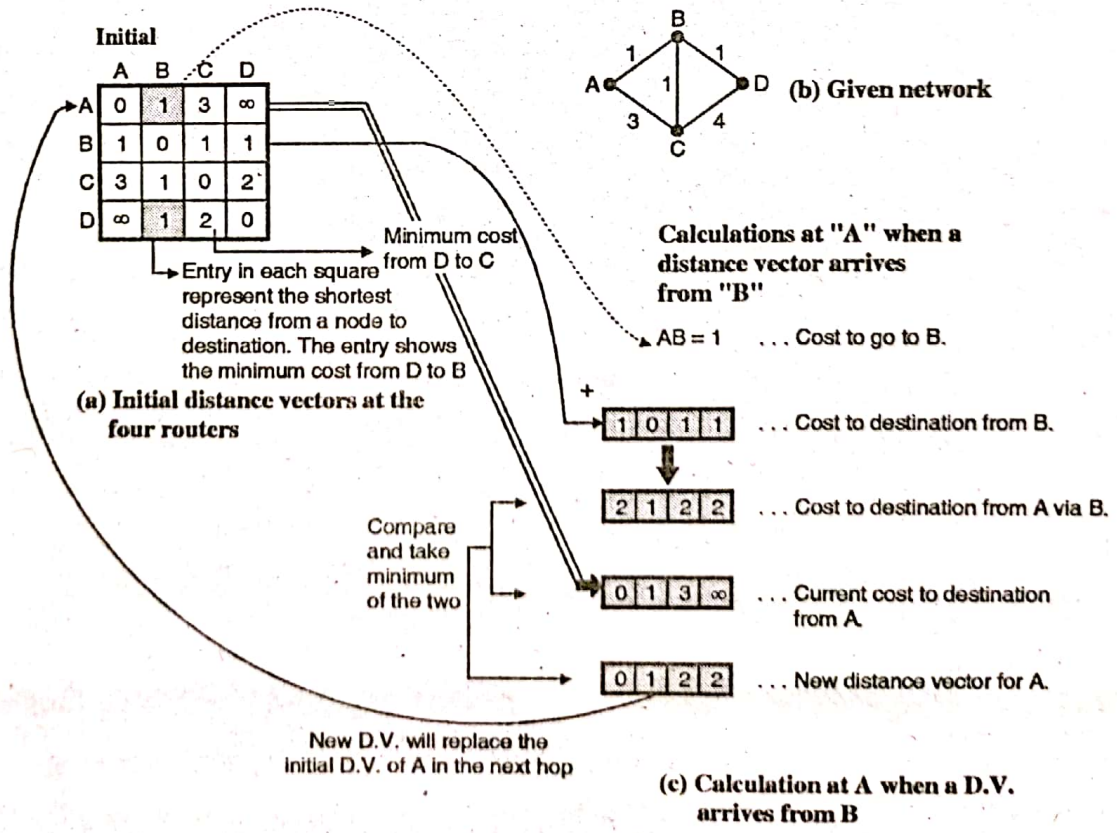
1. If the neighbouring node (say n) is not there in T then add it annotating it with the cost to reach it through p and p's ID.
2. If n is already present in T and the path to n through p has a lower cost, then remove the earlier instance of n and add the new instance annotated with the cost to reach it through p and p's ID.
3. Pick up the neighbour n which has the smallest cost in T, and if it is not present in P then add it to P. Use its annotation to determine the router p to use to react n.
4. Stop when T is empty.

Q. 18 Explain distance vector routing and its count to infinity problem.

May 07, Dec. 07, May 11, May 12, Dec. 12, May 17

Ans. :

In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there.



(G-463) Fig. 5.8 : Distance vector algorithm at router A

Scanned by CamScanner

This algorithm is sometimes called by other names such as :

1. Distributed Bellman-Ford routing algorithm.
2. Ford-Fulkerson algorithm

In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet. This entry has two parts :

1. The first part shows the preferred outgoing line to be used to reach the specific destination.
2. Second part gives an estimate of the time or distance to that destination.

Distance vector :

In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known. A **distance vector** is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance vector.

The cost in each tuple is equal the sum of costs on the shortest path to the destination.

Updation of router tables :

A router periodically sends a copy of its distance vector to all its neighbours. When a router receives a distance vector from its neighbour, it tries to find out whether its cost to reach any destination would decrease if it routed packets to that destination through that particular neighbouring router. This is illustrated in Fig. 5.8.

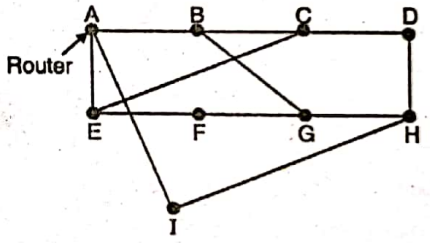
Fig. 5.8 shows how the D.V. at A is automatically modified when a D.V. is received from B. A similar calculation takes place at the other routers as well. So the entries at every router can change. In Fig. 5.8(a) the initial distance vector is shown. The entries indicate to the costs corresponding to the shortest distance between the routers indicate to that square.

For example, AC = 3 indicates the cost corresponding to the shortest path in terms of number of hops from A to C. Even if nodes asynchronously update their distance vectors the routing tables eventually converge.

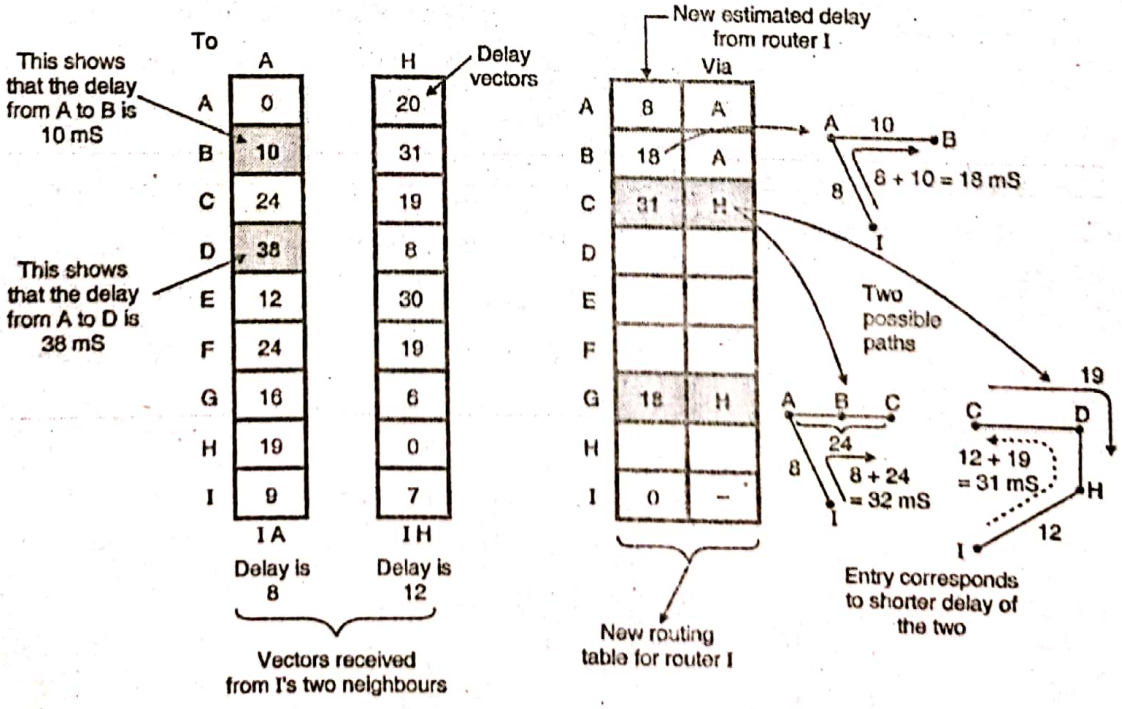
The well known example of distance vector routing is the Bellman-Ford algorithm.

Routing procedure in distance vector routing :

The example of a subnet is shown in Fig. 5.8(a) and the routing tables are shown in Fig. 5.8(b).



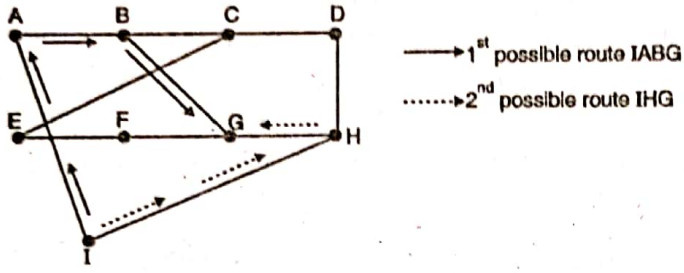
(G-464) **Fig. 5.8(a) : A subnet**



(G-465) **Fig. 5.8(b) : Routing tables**

Scanned by CamScanner

The entries in router tables of Fig. 5.8(b) are the delay vectors. For example consider the shaded boxes of Fig. 5.8(b). The entry in the first shaded box shows that the delay from A to B is 10 msec, whereas the entry in the other shaded box indicates that the delay from A to D is 38 msec. Consider how router I computes its new route to router G. Fig. 5.8(c) shows the two possible routes between I and G.



(G-466) **Fig. 5.8(c)**

I knows that the reach G via A, the delay required is :

(L-891)

I to A Delay = 8mS
A to G Delay = 16mS
$\therefore$ I to G Delay = 8 + 16 = 24 msec

Whereas the delay between I and G via H (route IHG) is :

(L-892)

I to H Delay = 12mS
H to G Delay = 6mS
$\therefore$ I to G Delay = 12 + 6 = 18 msec

The best of these values is 18 msec corresponding to the path IHG. Hence it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H. The new routing table for router I is shown in Fig. 5.8(b).

Similarly we can calculate the delays, from I to different destinations from A to I and enter the minimum possible delay into the I's router table.

Disadvantages :

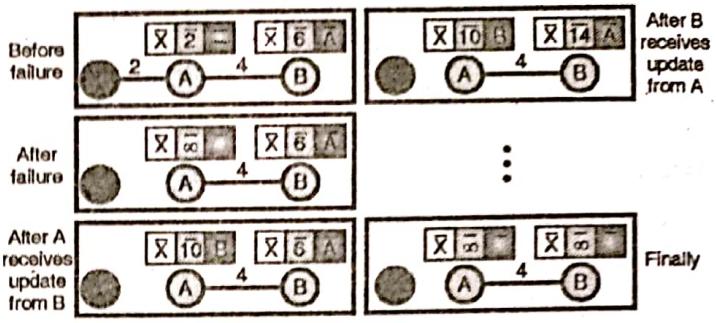
1. The distance vector routing takes a long time in converging to the correct answer. This is due to a problem called count-to-infinity problem. This problem can be solved by using the split horizon algorithm.
2. Another problem is that this algorithm does not take the line bandwidth into consideration when choosing a root. This is a serious problem due to which this algorithm was replaced by the Link State Routing algorithm.

Looping in distance vector routing protocol :

A problem in distance vector rooting is its instability. A network using this protocol can become unstable.

Two node loop instability :

A network with three nodes has been shown in Fig. 5.8(d).



(G-1499) **Fig. 5.8(d) : Two node loop instability**

At the beginning both nodes A and B know how to reach node X. But the link joining A and X fails suddenly. So node A changes its table. If A could send its changed routing table to B immediately, everything is okay. No problem will occur. But the system becomes unstable if B sends its routing table to A before receiving A's routing table.

This is because node A receives the updated B's routing table and assumes that B has found a new path to reach node X. So A immediately updates its routing table (which is incorrect). Based on this update now A sends its new update to B. Now B thinks that something has changed around A and so it updates its routing table.

Due to this process, the cost of reaching X increases gradually and finally becomes infinite. At this moment both A and B understand that now it is impossible to reach X. Note that during this entire time the system is unstable. A thinks that the route to X goes via B whereas B thinks that the route is via node A.

So if A receives a packet for X, it goes to B and then again returns back to A. Similarly if B receives a packet destined for X, it goes to A and returns back to B. This bouncing of packets between nodes A and B is known as the **two-node loop problem.**

This problem can be solved by using one of the following strategies :

1. Defining infinity
2. Split horizon
3. Split horizon and poison reverse.

There is a similar problem called three node loop problem present in the system using distance vector routing.

Q. 19 Explain count-to-infinity problem with the help of an example. It is a drawback of which algorithm.

Dec. 04, Dec. 09, May 10, May 11, May 15, May 17

Ans. :

Theoretically the distance vector routing works properly but practically it has a serious problem. The problem is that we get a correct answer but we get it slowly. In other words it reacts quickly to good news but it reacts too slowly to bad news.

Consider a router whose best route to destination X is large. If on the next exchange neighbour. A suddenly reports a short delay to X, the router will switch over and start using the line to A

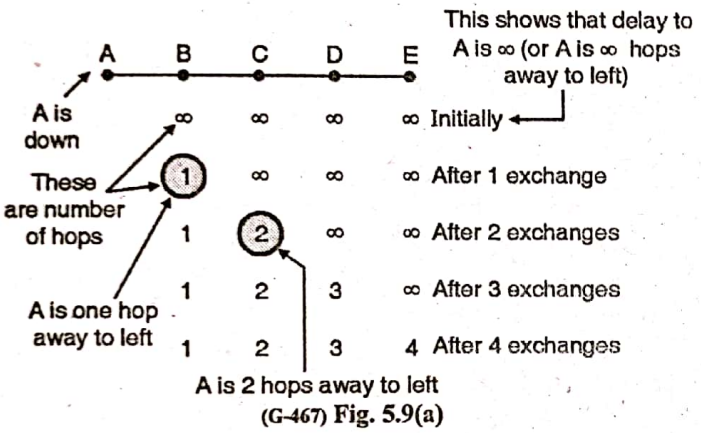
Scanned by CamScanner

for sending the traffic to destination X. Thus in one vector exchange, the good news is processed.

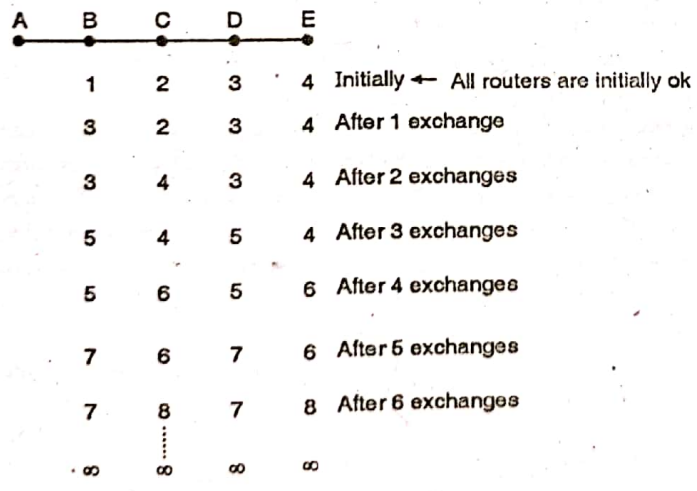
Consider a linear subnet of Fig. 5.9 which has five nodes. The delay metric used is the number of hops. Assume that A is initially down and that all the other routers know this. So all the routers have recorded that the delay to A is infinity.

When A becomes OK, the other routers come to know about it via the vector exchanges. Then suddenly a vector exchange at all the routers will take place simultaneously. At the time of first vector exchange, B comes to know that its left neighbour has a zero delay to A. So as shown in Fig. 5.9(a). B makes an entry in its routing table that A is one hop away to the left. All the other routers still think that A is down. So in the second row of Fig. 5.9(a), the entries below C D E are ∞.

On the second vector exchange, C comes to know that B has a path of 1 hop length to A, so C updates its routing table and indicates a path of 2 hop length. But D and E do not change their table entries.

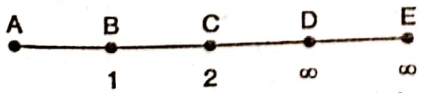


(G-467) **Fig. 5.9(a)**



(G-468) **Fig. 5.9(b)**

So after the second vector exchange the entries in the third row of Fig. 5.9(a) are :



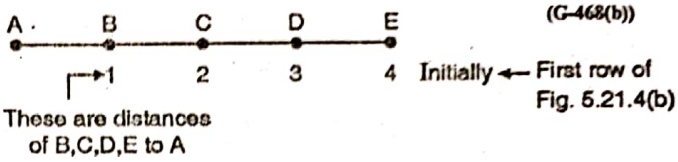
(G-468(a))

Similarly D and E will update their routing tables after 3 and 4 exchanges respectively.

So we conclude that the good news of A has recovered has spread at a rate of one hop per exchange.

Explanation of Fig. 5.9(b) :

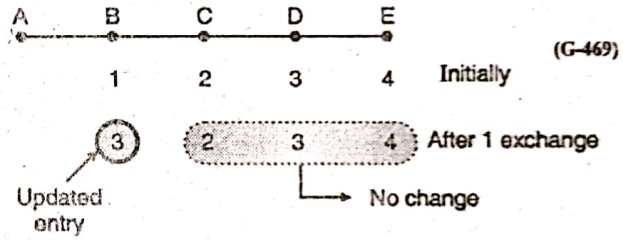
Now refer Fig. 5.9(b). Here initially all routers are OK. The routers B, C, D and E have distances of 1, 2, 3 and 4 respectively to A. So the first row of Fig. 5.9(b) is as follows :



(G-468(b))

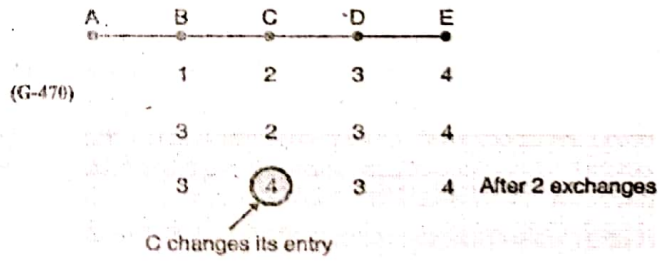
Now imagine that suddenly A goes down or line between A and B is cut. At the first packet exchange B does not hear anything from A (because A is down). But C says " I have a path of length 2 to A". But poor B does not understand that this path is through B itself. So B thinks that it can reach A via C with a path length

3. (B to C 1 hop and C to A 2 hops) so it accordingly updates its routing table. But D and E do not update their entries. So the second row of Fig. 5.9(b) looks as follows :



(G-469)

On the second exchange C realizes that both its neighbours (B and D) claim to have a path of length 3 to A. So it picks one of them at random and makes its new distance to A as 4. This is shown in row 3 of Fig. 5.9(b). It is repeated below.



(G-470)

Similarly the other routers keep updating their tables after every exchange. It is expected that finally we should get ∞ in the router tables of B, C, D and E indicating that A is down. We do reach this state at the end in Fig. 5.9(b) but after a very long time. The conclusion is bad news propagates slowly. This problem is called as **count-to-infinity** problem.

The solution to this problem is to use the split horizon algorithm.

Q. 20 What are the steps involved in link state routing. Explain the contents and the requirements of link state packets. Dec. 13, May 16, Dec. 16

Scanned by CamScanner

Ans. :

Distance vector routing was used in ARPANET upto 1979. After that it was replaced by the link state routing. Variants of this algorithm are now widely used. The link state routing is simple and each router has to perform the following five operations.

Router operations :

1. Each router should discover its neighbours and obtain their network addresses.
2. Then it should measure the delay or cost to each of these neighbours.
3. It should construct a packet containing the network addresses and the delays of all the neighbours.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router. Then a shortest path algorithm such as Dijkshtra's algorithm can be used to find the shortest path to every other router.

Protocols :

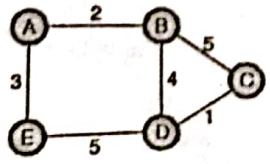
Link state routing is popularly used in practice. The OSPF protocol which is used in the Internet uses the link state algorithm.

IS-IS i.e. Intermediate system – Intermediate system is the other protocol which uses the link state algorithm. IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

Building a routing table in link state routing :

Link state routing :

Now we will see the development of routing table in link state routing. Here the term **link state** is used for defining the characteristic of a link or edge, which represents a network in the Internet. The **cost** associated with each link is important. The links having lower costs are preferred to the links having higher costs. A non-existing or broken link is indicated by an ∞ cost. In this method, each node must have a complete map of the network. That means each node should have complete information about the state of each link. The collection of states of all the links in an Internet is called as **Link-State Database (LSDB).** For the entire Internet, there is only one LSDB and its copy is available with each node. Each node uses it to create the least cost tree. The example of LSDB is as shown in Fig. 5.10(b) for the Internet shown in Fig. 5.10(a). The next step is creation of LSDB (which contains all the information about the Internet) at each node.



(a) Internetwork

	A	B	C	D	E
A	0	2	∞	∞	3
B	2	0	5	4	∞
C	∞	5	0	1	∞
D	∞	4	1	0	5
E	3	∞	∞	5	0

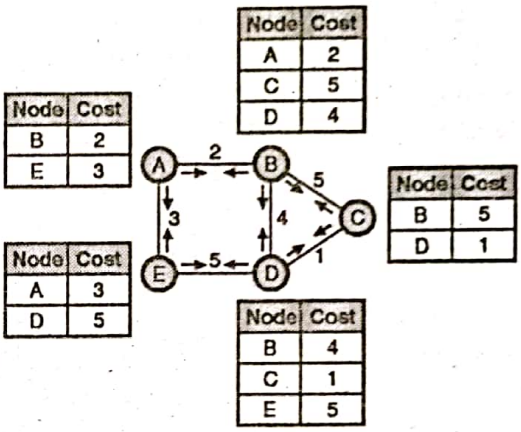
(b) Link state database (LSDB)

(G-2201) Fig. 5.10

This can be achieved by a process called **flooding.** Each node sends a greeting message to all its immediate neighbours, so as to collect two important pieces of information as follows :

1. The identity of the neighbouring node. 2. Cost of the link.

The packet containing this information is called as **LS Packet** (LSP), which is sent out of each interface. After receiving all the new LSPs each node will create the comprehensive LSDB as shown in Fig. 5.10(c). This LSDB is same for each node which shows the whole map of the internet. That means a node can use the LSDB to make the whole map of the Internet.



(G-2202) Fig. 5.10(c)

Q. 21 When would we prefer to use hierarchical routing over link state routing ? Explain.

Dec. 13, Dec. 15

Ans. :

As the size of the network increases, the size of the routing tables of the routers also increases. As a result of large routing tables, the router memory is consumed to a great extent, more CPU time is needed to scan the tables and more bandwidth is required to send status report about the tables. Sometimes the network becomes so large that the size of the router table becomes excessively large and practically it becomes impossible for every router to have an entry for all the other routers except itself. Then the hierarchical routing such as the one used in telephone networks should be used. In this type of routing the total number of routers are divided into different **regions.** A router will know everything about the all other belonging to its own region only. It does not know anything about the internal structure of other regions. This reduces the size of the router table. When various networks are connected together, each network is treated as a separate region. For very large networks the hierarchy is prepared as follows :

Level 1 : Regions

Level 2 : Clusters : It is a group of regions.

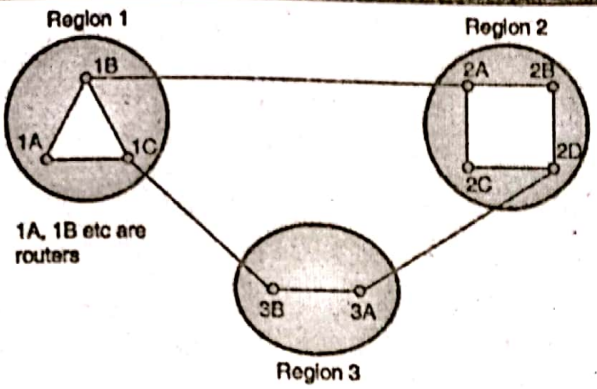
Level 3 : Zones : Zone is a group of clusters.

Level 4 : Groups : Group contains many zones.

Two level hierarchical routing :

For networks of smaller size, a two level hierarchical routing is sufficient. Fig. 5.11(a) shows network containing 3 regions. Fig. 5.11(b) shows the full routing table of router 1A which has 9 entries because in all there are 9 routers.

Scanned by CamScanner



(G-471) **Fig. 5.11(a) : A network**

Full routing table for 1A

Destination	Line	Hops
1 A	–	–
1 B	1 B	1
1 C	1 C	1
2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

(G-2304) **Fig. 5.11(b) : Full routing table for router 1A**

Now with a two level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in Fig. 5.11(c). This table has only 5 entries.

Hierarchical routing table for 1A

Destination	Line	Hops
Region 1 — 1 A	–	–
Region 1 — 1 B	1 B	1
Region 1 — 1 C	1 C	1
Region 2 → 2	1 B	2
Region 3 → 3	1 C	2

(c) Hierarchical routing table for router 1A

(G-2305) **Fig. 5.11**

In the hierarchical table of Fig. 5.11(c), there are entries for all local routers (1 A, 1 B and 1 C) belonging to the region of 1 A as before. But there are no detailed entries for the other regions.

Instead all other regions have been compressed into a single router per region. For example traffic from 1A to any router in region-2 is via 1 B-2 A line as shown by the shaded entry in Fig. 5.11(c). Similarly all the traffic from 1A to region 3 is routed through the line 1C-3B. Comparison of Figs. 5.11(b) and (c) shows how hierarchical routing reduces the size of routing tables.

Disadvantage : The reduced table size has a price tag attached to it. It comes at the expense of increased path length. But it is practically acceptable.

How many levels a hierarchy should have ?

Kamoun and Kleinrock have discovered that for an N router subnet, the optimum number of hierarchy levels is $\log_e N$ and it requires a total of $\log_e N$ entries per router table.

Q. 22 Explain with example MAC address.

May 08, May 09, Dec. 15

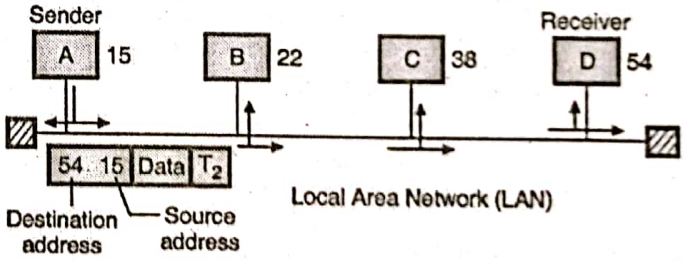
Ans. :

The packets from source to destination hosts pass through physical networks. At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses. A MAC address is a local address. It is unique locally but it is not unique universally. The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time.

Similarly a packet may pass through different physical networks. So to deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.

Most importantly we should be able to map the IP address into a corresponding MAC address. The size and format of the physical address varies depending on the nature of network. The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is imprinted on the network interfacing card (NIC).

Refer Fig. 5.12 which explains the concept of physical addressing.



(G-77) **Fig. 5.12 : Physical addresses**

The sender computer with a physical address of 15 wants to communicate with the receiver computer with a physical address 54. The frame sent by the sender consists of the destination address, sender's address, encapsulated data and a trailer (T_2) that contains the error control bit. When this frame travels over the bus topology, every computer receives it and tries to match it with its own physical address. If the destination address in the frame header does not match with the physical address it will simply drop the frame.

At receiver computer (D), the destination address matches with its physical address (54). So the frame is accepted and decapsulation is carried out to recover the data. The example of a

Scanned by CamScanner

48 bit or 6 byte physical address is as follows. It contains 12-hexadecimal digits.

08 : 63 : 4C : 81 : 08 : 1D

Q. 23 Explain logical Addresses. Dec. 15

Ans. :

Logical addresses are required to facilitate universal communications in which different types of physical networks can be involved. The logical address is also called as the IP (Internet Protocol) address. The internet consists of many physical networks interconnected via devices like routers.

Internet is a packed switched network that means the data from the source computer is sent in the form of small packets carrying the destination address upon them. A packet starts from the source host, passes through many physical networks and finally reaches the destination host. At the network level, the hosts and routers are recognized by their **IP addresses.** or logical addresses.

An IP address is an internetwork address. It is a universally unique address. Every protocol involved in internetworking requires IP addresses. The logical address used in internet is currently a 32-bit address. The same IP address can never be used by more than one computer on the Internet.

Q. 24 Explain Mapping of IP Address to a MAC Address. Dec. 15

Ans. :

We have seen the need of mapping an IP address into a MAC address. Such a mapping can be of two types :

1. Static mapping and 2. Dynamic mapping

1. Static mapping :

In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address. If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table. The limitation of static mapping is that the MAC addresses can change. These changed MAC addresses must be updated periodically in the static mapping table.

2. Dynamic mapping :

In dynamic mapping technique a protocol is used for finding the other address when one type of address is known. There are two protocols used for carrying out the dynamic mapping. They are :

1. Address Resolution Protocol (ARP).
2. Reverse Address Resolution Protocol (RARP)

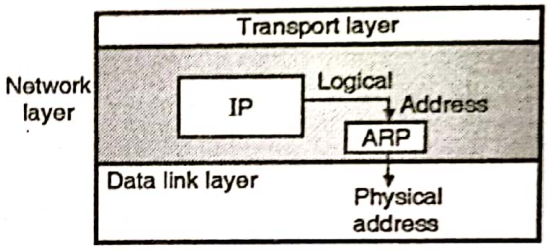
The ARP is used for mapping an IP address to a MAC address whereas the RARP is used for mapping a MAC address to an IP address.

Q. 25 Write short note on Address Resolution Protocol (ARP). May 04, May 15

Ans. :

If a host or a router wants to send an IP datagram to another host or router, it has the IP address of the receiving host or router. But this IP datagram is going to be encapsulated in a frame (data link layer) so as to make it capable of passing through the physical network. For this the sender must know the physical address of the receiver.

The position of ARP in the TCP/IP suite has been shown in Fig. 5.13. It shows that IP sends the logical address to ARP which maps the logical address into its corresponding physical address and passes it to the data link layer.



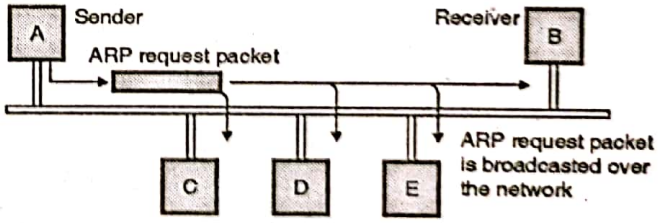
(G-2093) **Fig. 5.13 : Position of ARP in TCP / IP suite and its principle of operation**

ARP is used for mapping an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is stored on the NIC (Network Interface Card) of that machine.

How to find the MAC address ?

When a router or a host (A) needs to find the MAC address of another host (B) the sequence of events taking place is as follows :

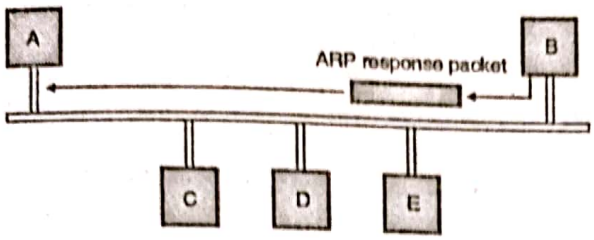
1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
2. This request packet is broadcasted over the network as shown in Fig. 5.13(a).



(G-575)**Fig. 5.13(a) : ARP request is broadcast**

3. Every host and router on the network will receive the ARP request packet and process it. But only the intended receiver (B) will recognize its IP address in the request packet and will send an ARP response packet back to A.
4. The ARP response packet has the IP and physical addresses of the receiver (B) in it. This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in Fig. 5.13(b). Thus host A has obtained the MAC address of B using ARP.

Scanned by CamScanner



(G-576) **Fig. 5.13(b) : ARP response unicast**

Q. 26 Write short note on : RARP. Dec. 04, Dec. 16

Ans. :

ARP is used for solving the problem of finding out which Ethernet address corresponds to a given IP address. That means ARP is used for the mapping of IP address to physical or MAC address. But sometimes we have to solve a reverse problem. That means we have to obtain the IP address corresponding to the given Ethernet (MAC) address. Such a problem can occur when booting a diskless workstation.

The problem of obtaining the IP address when an Ethernet address is given, can be solved by using RARP (Reverse Address Resolution Protocol). The newly booted workstation is allowed to broadcast its Ethernet address. The RARP server after receiving this request, checks the Ethernet address in its files and finds the corresponding IP address. This IP address is then sent back. The disadvantage of RARP is that it uses a destination address of all 1s (limited broadcasting) to reach the RARP server. But such broadcasts are not forwarded by routers, so a RARP server is needed on each network.

In order to get around this problem, another bootstrap protocol called BOOTP has been invented. Unlike RARP, it uses UDP messages which are forwarded over routers. It also provides a diskless workstation with additional information, including the IP address of the file server holding the memory image, the IP address of the default router and the subnet mask to use.

Q. 27 What is ICMP protocol ? Explain the ICMP header format with diagram. Dec. 16

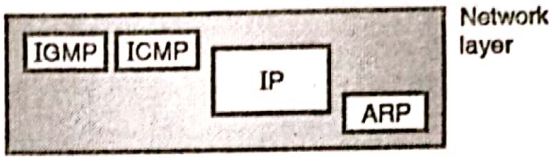
Ans. :

The IP provides unreliable and connectionless datagram delivery, and makes an efficient use of network resources. IP is a best-effort delivery (which does not provide any guarantee) service that takes a datagram from its original source to its final destination. However, IP has two drawbacks :

1. It does not have any error control mechanism.
2. It does not have any assistance mechanism.

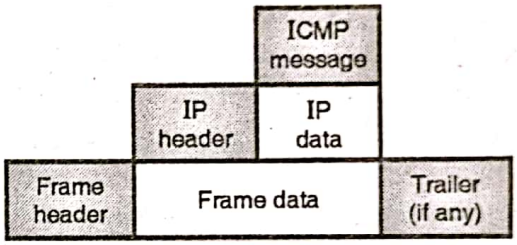
The Internet Control Message Protocol (ICMP) is used to overcome these drawbacks. It is used alongwith IP. It reports presence of errors and sends the control messages on behalf of IP. ICMP does not attempt to make IP a reliable protocol.

It simply attempts to report errors and provide feedback on specific conditions. ICMP messages are carried as IP packets and are therefore unreliable. ICMP is a network layer protocol. IP also lacks a mechanism for host and management queries. A host sometimes wants to know if a router or another host is operating or dead. And sometimes a network manager needs information from another computer on the network (such as host or router). Fig. 5.14 shows the position of ICMP with respect to the IP and other protocols in the network layer.



(G-2102) **Fig. 5.14 : Position of ICMP**

There are two versions of ICMP protocol namely ICMPv4 and ICMPv6. ICMP operates in the network layer but its messages are not passed directly to the data link layer. Instead, the messages are first encapsulated inside IP datagrams and then sent to the lower layer. This is as shown in Fig. 5.14(a).



(G-2103) **Fig. 5.14(a) : ICMP encapsulation**

The ping command uses ICMP as a probe to test whether a station is reachable. Ping packages an ICMP echo request message in a datagram and sends it to a selected destination. The user chooses the destination by specifying its IP address or name on the command line in a form such as :

ping 100.50.25.1

When the destination receives the echo request message, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times. If no reply arrives, ping indicates that the destination is unreachable. Another utility that uses ICMP is trace route, which provides a list of all the routers along the path to a specified destination.

Q. 28 Write short note on : IPv6. Dec. 07, Dec. 08, Dec. 10

Ans. :

IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4. IPv6 was designed to enable high-performance and larger address space. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.

Advantages of IPv6 :

1. Improved header format :

IPv6 uses an improved header format. In its header format the options are separated from the base header. These options are inserted when needed, between the base header and upper layer

Scanned by CamScanner

data. The routing process is simplified due to this modification. The speed of the routing process increases and the routing time is reduced.

2. Larger address space :

IPv6 has 128-bit address, which is 4 times wider in bits is compared to IPv4's 32-bit address space. So there is a large increase in the address space.

Address space of IPv6 = (2^{128})

3. New options :

IPv6 has increased functionality due to the addition of entirely new options that are absent in IPv4.

4. More security :

IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH : Authentication Header) for enhancing the security.

5. Possibility of extension :

The design of IPv6 is done in such a way that there is a possibility of extension of protocol if required.

6. Support to resource allocation :

To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification. With flow label mechanism, routers can recognize to which end-to-end flow the given packet belongs to.

7. Plug and play :

IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.

8. Clearer specification and optimization :

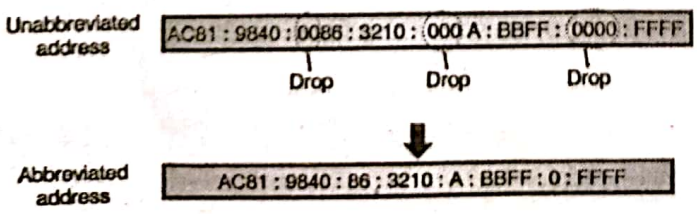
IPv6 follows good practices of IPv4, and omits flaws/obsolete items of IPv4.

Q. 29 Explain Classless Inter Domain Routing (CIDR).

Dec. 09, May 11, May 13

Ans. :

The IPv6 address, in hexadecimal format contains 32 digits and it is very long. But in this address many hex digits are zero. We can take advantage of this to shorten the address by abbreviating it. A section corresponds to four digits between any two colons. The leading zeros in a section can be omitted to reduce the length of the address as shown in Fig. 5.15.

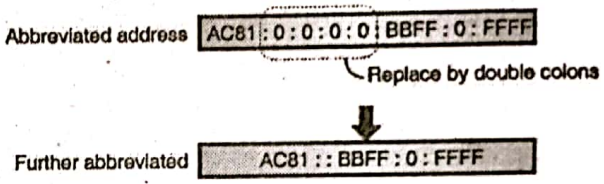


(G-546) **Fig. 5.15 : Abbreviated address**

Note that only the leading zeros can be dropped but the trailing zeros can not be dropped. This is illustrated in Fig. 5.15. Thus due to abbreviation the length of the address has reduced to 24 hex digits from 32.

Further abbreviation :

We can make further abbreviation if there are consecutive sections consisting of only zeros. This is known as **zero compression.** We can remove the zeros completely and replace them with double colon as shown in Fig. 5.15(a).



(G-547) **Fig. 5.15(a) : Further abbreviation (Zero compression)**

This further abbreviation has reduced the address length to just 13 hex digits. It is important to note that abbreviation can be done only once per address. Also note that if there are two sets of zero sections, then only one of them can be abbreviated.

3. Mixed representation :

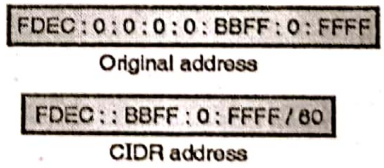
Sometimes, the IPv6 address is represented using a mixed representation which combines the **colon hex** and **dotted decimal** notations.

This notation is appropriate during the transition time during which an IPv4 address is being embedded in IPv6 address. In the mixed representation the rightmost 32 bits correspond to the IPv4 address Hence they are represented by the dotted decimal notation.

Whereas the leftmost 96 bits (6 sections) are represented in colon hex notation.

4. CIDR notation :

The type of addressing used in IPv6 is **hierarchical addressing.** Therefore IPv6 allows classless addressing and CIDR notation. Fig. 5.15(b) illustrates the CIDR address with a 60 bit prefix., how we can divide an IPv6 address into a prefix and a suffix.



(G-2132) **Fig. 5.15(b) : CIDR address**

Q. 30 Compare the network layer protocols IPv4 and IPv6.

Dec. 14

Ans. :

IPv4	IPv6
In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)

Scanned by CamScanner

IPv4	IPv6
The IPv4 address is written by dotted-decimal notation, e.g. 121.2.8.12	IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98: 5432:4567.
The basic length of the IPv4 header comprises a minimum of 20 bytes (without option fields). The maximum total length of the IPv4 header is 60 bytes (with option fields), and it uses 13 fields to identify various control settings.	The IPv6 header is a fixed header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
IPv4 header has a checksum, which must be computed by each router	IPv6 has no header checksum because checksums are, for example, above the TCP/IP protocol suite, and above the Token Ring, Ethernet, etc.
IPv4 contains an 8-bit field called Service Type. The Service Type field is composed of a TOS (Type of Service) field and a procedure field.	The IPv6 header contains an 8-bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets
The IPv4 node has only Stateful auto-configuration.	The IPv6 node has both a stateful and a stateless address autoconfiguration mechanism.
Security in IPv4 networks is limited to tunneling between two networks	IPv6 has been designed to satisfy the growing and expanded need for network security.
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Header includes options	All optional data is moved to IPv6 extension headers.

Q. 31 An ISP is granted a block of addresses starting with 150.80.0.0/16.

The ISP wants to distribute these blocks to 2600 customers as follows :

a. The first group has 200 medium-size businesses ; each needs 128

b. The second group has 400 small businesses ; each needs 16

c. The third group has 2000 households ; each needs 4 addresses.

Design the subblocks and give the slash notation for each subblock. Find out how many addresses are still available after these allocations ? May 16

Ans. :

Granted address : 150.80.0.0/16

As n = 16 the total number of available addresses is $2^{32-n} = 2^{16} = 65536$.

The three groups are as follows :

Group 1 :

For this group each business needs 128 addresses. This means that 7 bits ($\log_2 128 = 7$) are required to define each host. The prefix length is then 32 – 7 = 25 i.e. $n_1 = 25$.

The addresses in group-1 are

1st business : 150.80.0.0/25 to 150.80.0.127/25

2nd business : 150.80.0.128/25 to 150.80.0.255/25

.

.

.

200th business : 150.80.99.128/25 to 150.80.99.255/25

Total addresses in group-1 = 200 × 128 = 25600

Group 2 :

For this group each business needs 16 addresses. Therefore 4 bits ($\log_2 16 = 4$) are required to define each host. The prefix length is then 32 – 4 = 28. i.e. $n_2 = 28$.

The addresses in group-2 are

1st business : 150.80.100.0/28 to 150.80.100.15/28

2nd business : 150.80.100.16/28 to 150.80.100.31/28

.

.

Scanned by CamScanner

400th business : 150.80.124.240/28 to 150.80.124.255/28

Total addresses in group-2 = 400 × 16 = 6400

Group 3 :

For this group each household needs 4 addresses. Therefore only 2 bits ($\log_2 4 = 2$) are required to define each host.

The prefix length is then 32 – 2 = 30 i.e. $n_3 = 30$

The addresses of group-3 are

1st household : 150.80.125.0/30 to 150.80.125.3/30

2000th household : 150.80.156.60/30 to 150.80.156.63/30

Total addresses in group-3 = 2000 × 4 = 8000

Number of granted address to ISP = 65, 536

Number of allocated addresses by

ISP = 25600 + 6400 + 8000 = 40,000

Number of available addresses = 65, 536 – 40,000 = 25,536.

Q. 32 An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows :

1. **The first group has 64 customers ; each needs 256 addresses.**
2. **The second group has 128 customers ; each needs 128 addresses.**
3. **The third group has 128 customers ; each needs 64 addresses. Design the sub blocks and find out how many addresses are still available after these allocations.** Dec. 16

Ans. :

Group 1 :

Each customer in this group needs 256 addresses i.e. suffix length is 8 ($2^8 = 256$).

∴ Prefix length = 32 – 8 = 24. The addresses are as follows :

Customer	Starting address	Ending address
1.	190.100.0.0/24	190.100.0.255/24
2.	190.100.1.0/24	190.100.1.255/24
3.	190.100.2.0/24	190.100.2.255/24
.		
.		
.		
64	190.100.63.0/24	190.100.63.255/24

Total : 64 × 256 = 16384

Group 2 :

Each customer in this group needs 128 addresses i.e. suffix length is 7 ($2^7 = 128$).

∴ Prefix length = 32 – 7 = 25. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.64.0/25	190.100.64.127/25
2.	190.100.64.128/25	190.100.64.255/25
.		
.		
.		
128	190.100.127.128/25	190.100.127.255/25

Total : 128 × 128 = 16384

Group 3 :

Each customer in this group needs 64 addresses i.e. suffix length is 6. ($2^6 = 64$).

∴ Prefix length = 32 – 6 = 26. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.128.0/26	190.100.128.63/26
2.	190.100.128.64/26	190.100.128.127/26
.		
.		
.		
128	190.100.159.192/26	190.100.159.255/26

Total = 128 × 64 = 8192

Number of granted addresses to the ISP = 65536

Number of allocated addresses by the ISP = 40960

Number of available addresses = 65536 – 40960

= 24576

Q. 33 Why there is a need for congestion control ? What are the different mechanisms ? Explain them. Dec. 14

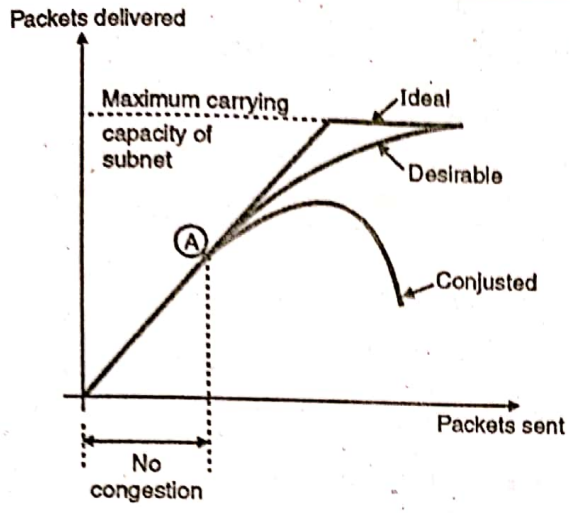
Ans. :

An important issue in a packet switching network is congestion. If an extremely large number of packets are present in a part of a subnet, the performance degrades. This situation is called as congestion. Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network (i.e. the number of packets a network can handle).

Fig. 5.16 explains the concept of congestion graphically. Upto point A in Fig. 5.16, the number of packets sent into the subnet by the host is within the capacity of the network. So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place. But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.

As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens. At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.

Scanned by CamScanner



(G-473) **Fig. 5.16 : Concept of congestion**

Need of Congestion Control :

It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.

Congestion will result in long queues, which results in buffer overflow and loss of packets. So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

Q. 34 Compare congestion control and flow control.

Dec. 08

Ans. :

Congestion control makes it sure that the subnet is able to carry the offered traffic i.e. the subnet is able to carry all the packets sent by all the senders to their destinations. Congestion control is dependent on the behaviour of all the hosts, all the routers and other factors which reduce the carrying capacity of a subnet.

On the contrary, the flow control is related to point to point traffic between a sender and its destination. Flow control ensures that a fast sender does not send data at a rate faster than the rate at which the receiver can receive it. Flow control involves some kind of feedback from the receiver, which can control the sending rate of the sender.

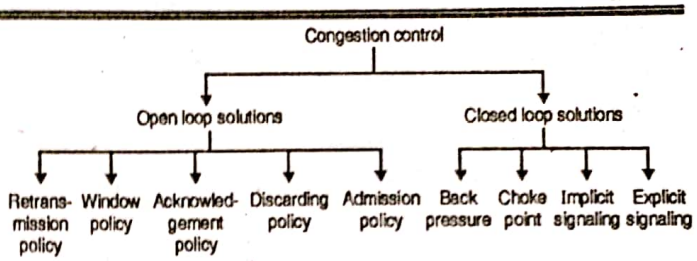
Q. 35 Write short notes on : Congestion control.

Dec. 05, Dec. 15, May 16, Dec. 16, Dec. 17

Ans. :

The solutions to the congestion problems can be divided into two categories or groups as open loop solutions and closed loop solutions. Congestion control refers to the techniques and mechanisms which can either prevent congestion from happening or remove congestion after it has taken place. The **open loop congestion** control is based on the prevention of congestion whereas the **closed loop solutions** are for removing the congestion after it has occurred.

Fig. 5.17 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-476) **Fig. 5.17 : Classification of congestion control schemes**

Open loop control :

Open loop solutions try to solve the congestion issue by excellent design to prevent the congestion from happening. Open loop control is exercised by using the tools such as deciding when to accept the new packets, when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points. It is important to note that none of these decisions are made on the basis of the current status of a network, as no feedback is being used.

Closed loop control :

The closed loop congestion control uses some kind of feedback. It takes into account the current status of the network. A closed loop control is based on the following three steps :

1. Detect the congestion and locate it by monitoring the system.
2. Transfer the information about congestion to places where action can be taken.
3. Adjust the system operations to correct the congestion.

Two examples of closed loop control are :

1. TCP flow control.
2. BR rate control for an ATM network.

Open loop versus closed loop :

Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control. In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.

Some people feel that closed loop congestion control schemes are too slow in today's high-speed, large range network. Because it takes a long time for feedback to go back to source. Hence before any corrective action takes place thousands of packets have been already lost. But on other hand, if the congestion has already taken place and the overload is of long duration, the congestion cannot be released unless the source causing the congestion is asked to reduce its rate. Furthermore, ABR service is designed to use any bandwidth that is left over the source must have some knowledge of what is available when it is sending cells.

Q. 36 Explain various congestion prevention policies.

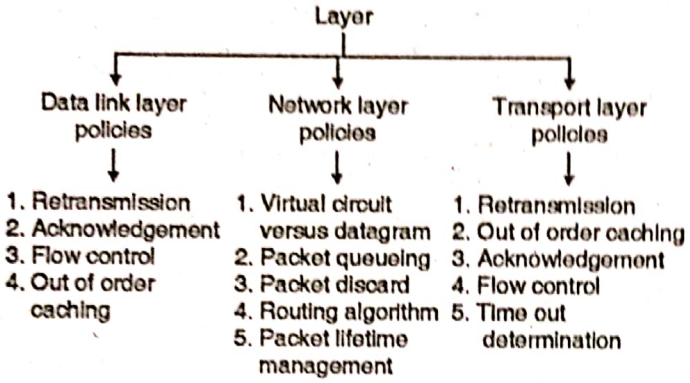
May 12, Dec. 12, Dec. 15, May 17, Dec. 17

Ans. :

The open loop congestion control systems. These systems try to avoid congestion by using the appropriate policies at different

Scanned by CamScanner

levels. Fig. 5.18 lists various policies corresponding to different layers for avoiding congestion.



(G-477) **Fig. 5.18 : Policies affecting the congestion**

Policies related to data link layer :

1. Retransmission policy :

The retransmission policy and the retransmission timers must be designed to optimise efficiency and at the same time prevent congestion.

The retransmission policy deals with how fast a sender times out. If a sender times out early then it will retransmit all the packets and such a retransmission can lead to congestion. By designing the retransmission policy we can avoid this and prevent congestion.

2. Out of order caching policy :

If the receivers routinely discard all the packets which are out of order, then retransmission of these packets will take place. This will increase the load and result in congestion. So a selective repeat (retransmission) should be adopted to avoid congestion.

3. Acknowledgement policy :

If each received packet is promptly acknowledged then the acknowledgement packets will increase the traffic. If the acknowledgement is delayed (piggybacking) then there is a possibility of time out and retransmission.

So a tight flow control has to be exercised to avoid congestion.

4. Window policy :

The type of window at the sender may also affect congestion. The selective repeat window is better than the Go Back N window.

Policies related to network layer :

1. Choice between virtual circuit and datagrams :

This choice at the network layer will affect the congestion because many congestion control algorithms work only with virtual circuit subnets.

2. Packet queuing and service :

This policy is related to whether the routers have one queue per input line and one queue per output line or both.

This policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.

3. Discard policy :

This policy lays a rule which tells the routers about which packet is to be discarded. A good discard policy can prevent congestion and a bad one will worsen the situation.

4. Routing algorithms :

The routing algorithms can spread the traffic over all the lines. By doing so it is ensured that none of the lines are overloaded. This will certainly avoid congestion.

5. Package lifetime management :

This policy decides the maximum time for which a packet may live before being discarded. This time should be of adequate value so that congestion can be avoided.

Policies related to transport layer :

The policies at the transport layer are same as those at the data link layer. But at transport layer determining the time out interval is more difficult. If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will reduce at the cost of increased response time (network will become slow).

Traffic shaping :

One of the important reason behind congestion is the bursty nature of the traffic. If the traffic has a uniform data rate then congestion would not happen every now and then. But due to bursty traffic it can happen regularly. Traffic shaping is an open loop control. It prevents the congestion by making the packet transmission rate to be more predictable (bursty traffic is unpredictable).Thus traffic shaping will regulate the average rate or the burstiness of data transmission. Monitoring a traffic flow is called as **traffic policing**. Check if a packet stream (connection) is as per its descriptor, and if it is not as per its descriptor, then give penalty ! In order to achieve this the network may want to monitor the traffic flow during the connection period. The process of monitoring and enforcing the traffic flow is called traffic policing. The types of penalties enforced are as follows :

1. Drop packets that violate the descriptor.
2. Give low priority to the packets violating the descriptor.

Q. 37 Explain the congestion control in virtual circuit and datagram subnets. May 12, Dec. 12, May 17

Ans. :

Admission control principle :

This technique is used to keep the congestion which has already begun to a manageable level and does not allow it to worsen any further. Its principle is as follows : Once congestion has been detected, do not set up any more virtual circuits until the

Scanned by CamScanner

congestion is cleared. The advantage of this technique is that it is a simple and easy to carry out control.

Alternative approach :

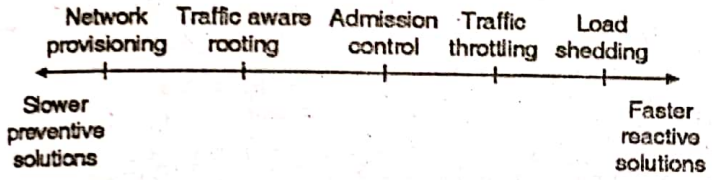
An alternative approach to admission control allows the virtual circuits to set up even when a congestion has taken place. But carefully route all the new virtual circuits around the area where congestion is already present.

Approaches to Congestion Control :

The two basic solutions to the problem of congestion are :

1. Increase the resources 2. Decrease the load

These solutions are applied on different time scales in order to either prevent congestion or handle it if it has occurred.



(G-1522) **Fig. 5.19 : Time scales of approaches to congestion control**

1. Network provisioning :

The fundamental way of avoiding congestion is to build a network that is properly matched to the traffic that it is going to carry. If the network uses a low bandwidth link along which a heavy traffic is directed, then congestion is most certain to take place. We can add resources dynamically when there is congestion. For example, we can turn on additional routers and use spare (back up) lines whenever congestion has taken place.

Another example is purchasing bandwidth on open market as and when congestion occurs. But you can't do it instantly. It takes a long time. This is called as **Network Provisioning.** It is a slow preventive solution and happens on a time scale of months.

2. Traffic aware routing :

If we cannot increase the capacity of a network then we should think of utilizing the existing capacity in the best possible why. Routers can be tailored to suite traffic patterns that change during the day as network users wake and sleep in different time zones. The traffic can be routed over those paths which have less traffic at that time. This is known as traffic aware routing.

3. Admission control :

Sometimes it is not possible to increase capacity. Then the only possible way to fight congestion is to **decrease the load.** In the virtual circuit networks, new connections are not allowed once congestion has been detected. This is a feedback (closed loop) control approach. When the congestion is predicted, the network can deliver feedback to those sources who are responsible for congestion. Then these sources would be requested to **reduce** their outputs. There are two difficulties faced in this approach :

1. It is difficult detect the of beginning of congestion.
2. It is also difficult to inform the sources to slow down accordingly.

The **leaky bucket** and **token bucket** methods are examples of admission control.

4. Traffic throttling (Congestion avoidance) :

In the Internet and many other computer networks, senders adjust their transmission rates and send only that much traffic which a network can readily deliver without causing congestion. This is done so as to operates the network just before the beginning point of congestion.

When congestion is about to happen the senders should be told to **reduce** their transmission and slow down. This technique is an example of **congestion avoidance** principle. The first step in traffic throttling is to **detect** the beginning point of congestion and the second step is to tell the senders to slow down. Note that traffic throttling approach can be used in both datagram **subnets** as well as **virtual circuit subnets.** The onset of congestion can be detected if the routers are made to monitor the following parameters :

1. Utilization of output links.
2. Buffering of queued packets inside the router.
3. Number of packets lost due to inadequate buffering.

Generally the second parameter is most useful in practice. The second task for the routers is that they should deliver timely feedback to the senders. Different schemes use different feedback mechanisms. Some of them are as follows :

1. Choke packets.
2. Explicit Congestion Notification (ECN).
3. Hop by Hop back pressure.

5. Load shedding :

When all other solutions fail to contain congestion, the network has no option but to discard packets that cannot be delivered. A good policy for selecting which packets to discard can help preventing the congestion collapse.

Q. 38 Explain the various methods for congestion control used in datagram subnets.

Dec. 04, May 12, Dec. 12, Dec. 13, Dec. 14, May 17

Ans. :

Now see some congestion control approaches which can be used in the datagram subnets (and also in virtual circuit subnets). The techniques are :

1. Choke packets 2. Load shedding 3. Jitter control.

1. Choke packets :

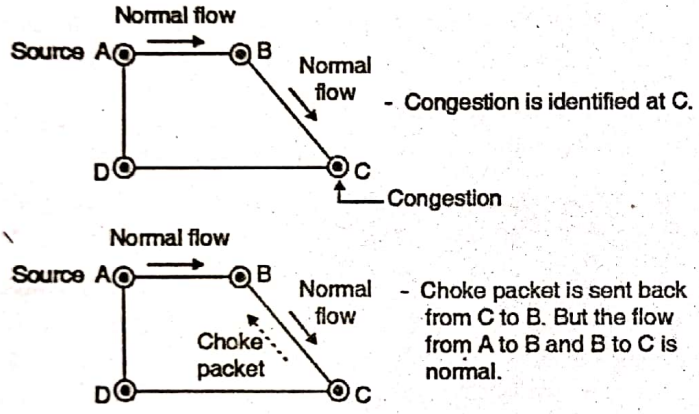
This approach can be used in virtual circuits as well as in the datagram subnets. In this technique each router associates a real

Scanned by CamScanner

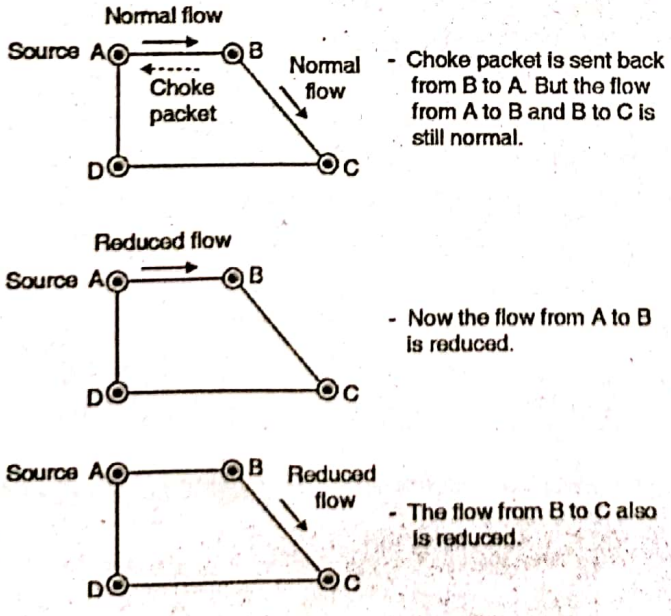
variable with each of its output lines. This real variable say "u" has a value between 0 and 1 and it indicates the how much is utilization of that line in percentage (60 %, 70 % etc.). If the value of "u" goes above the threshold then that output line will enter into a "warning" state. The router will check each newly arriving packet to see if its output line is in the "warning state".

If it is in the warning state then the router will send back a **choke packet** signal to the sending host. The sender host will not generate any more data packets. This will reduce the congestion. Different congestion control algorithm have been proposed, depending on the value of thresholds. Depending on the threshold value, the choke packets can contain a mild warning, a stern warning or an ultimatum.

Another algorithm may use the queue lengths or buffer utilization instead of using the line utilization as a deciding factor. The general concept of choke packet mechanism is demonstrated in Fig. 5.20(a).



(G-478) Fig. 5.20(a)



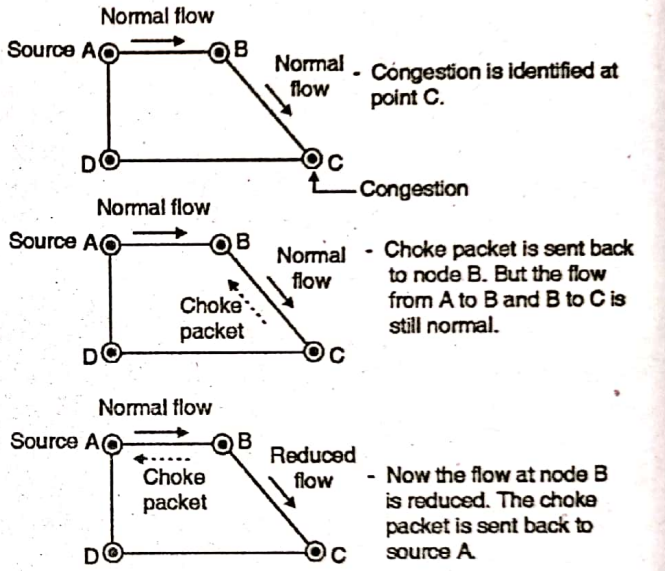
(G-478) Fig. 5.20(a) : Choke packet mechanism

Fig. 5.20(a) shows that, the choke packets have to travel over the entire network, from the point of congestion to the appropriate source (i.e. from C to A). Then the action of reducing the flow will take place. The whole process is therefore very much time consuming.

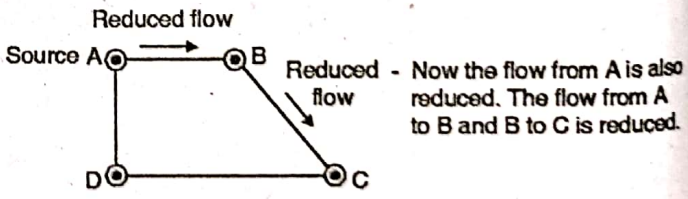
Hop-by-Hop choke packet technique :

The problem associated with the general choke packet mechanism can be overcome by using another technique called as hop-by-hop choke packet technique. This is demonstrated in Fig. 5.20(b). In this approach, the choke packets are used at each hop between the destination and source. Each node receiving the choke packet will reduce its output flow. This will have a more effective and fast control over the overall transmission rate.

Fig. 5.20(b) shows how the transmission rate is reduced at every hop in response to the choke packets.



(G-479) Fig. 5.20(b)(Contd...)



(G-479) Fig. 5.20(b) : Concept of hop-by-hop choke packet mechanism

Disadvantage :

The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is not compulsory. The host may reduce its transmission rate or ignore the choke packets.

Weighted fair queuing :

The disadvantage of choke packet technique can be overcome with the help of the weighted queuing technique. The queuing algorithm was proposed first in 1987. In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.

Scanned by CamScanner

2. Load shedding :

Admission control, choke packets, fair queuing are the techniques suitable for light congestion. But if these techniques cannot eliminate the congestion, then the load shedding technique is to be used. The principle of load shedding states that when the routers are flooded with the packets that they cannot handle, they should simply throw the packets away.

A router which is flooding with packets due to congestion can discard any packet at random. But there are better ways of doing this. The policy for dropping a packet depends on the type of packet. For file transfer an old packet is more important than a new packet. In contrast for multimedia a new packet is more important than an old one. Accordingly a policy is formulated for discarding the packets. An intelligent discard policy can be decided depending on the applications. It is not possible to implement such an intelligent discard policy without the, co-operation from the sender. The applications should mark their packets as per priority to indicate how important they are. If this is done then when the packets are to be discarded the routers can first drop packets having lower priority (i.e. the packets which are least important). Then the routers will discard the packets from next lower class and so on. One or more header bits are required to put the priority of a packet.

In every ATM cell, 1 bit is reserved in the header for marking the priority. Every ATM cell is labeled either as a low priority or high priority.

3. Jitter Control :

Definition :

The delay introduced by the data communication networks is not constant. It varies packet to packet. The jitter measures the variability in packet delays and it is measured in terms of the difference of the minimum delay and maximum value of delay.

Jitter is defined as the variation in delay for the packets belonging to the same flow. The real time audio and video cannot tolerate jitter on the other hand the jitter does not matter if the packets are carrying any data information contained in a file. For the audio and video transmission if the packets take 20 msec to 30 msec (delay) to reach the destination, it does not matter, provided that the delay remains constant. The quality of sound or video will be hampered if the delays associated with different packets have different values.

Jitter control :

When a packet arrives at a router, the router will check to see whether the packet is behind or ahead and by what time. This information is stored in the packet and updated at every hop. If the packet is ahead of the schedule (early) then the router will hold it for a slightly longer time and if the packet is behind the schedule (late), then the router will try to send it out as quickly as possible.

This will help in keeping the average delay per packet constant and will avoid time jitter.

Q. 39 Write short notes on : Quality of Service (QoS) of internetworking.

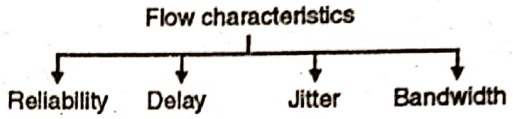
May 10, Dec. 10, May 11, May 13, Dec. 13

Ans. :

The long form of QoS is quality of service and it is an internetworking issue. We can informally define quality of service as something flow seeks to attain.

Flow characteristics :

There are four important characteristics of data flow : reliability, delay, jitter and bandwidth. These characteristics are shown in Fig. 5.21.



(G-480) **Fig. 5.21 : Flow characteristics**

1. Reliability :

A data flow must have some level of reliability. Lack of reliability means a packet or acknowledgment, will be lost and retransmission will be required. However, each application programs has a different demand for reliability. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

2. Delay :

Source-to-destination delay is another important flow characteristic. Again delay tolerance of different applications will be different. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while file transfer or email are delay tolerant applications.

3. Jitter :

Jitter is the variation in delay for packets belonging to the same flow. i.e. different packets experience different amounts of delays. Real-time audio and video cannot tolerate a large amount of jitter. On the other hand, it does not matter if packet carrying information in a file have different delays. The transport layer at the destination waits until all packets arrive before delivery to the application layer.

4. Bandwidth :

Different applications need different bandwidths. In video conferencing needs a huge bandwidth whereas an email may not need a large bandwidth.

Techniques for Achieving Good QoS :

Some of the techniques useful in achieving good QoS are as follows :

1. Buffering
2. Traffic shaping
3. Leaky bucket algorithm
4. Token bucket algorithm
5. Resource reservation
6. Admission control
7. Proportional routing
8. Packet scheduling.

Scanned by CamScanner

Q. 40 What is traffic shaping ? Explain leaky bucket algorithm. Dec. 06, May 09, May 10, Dec. 15

Ans. :

Definition of traffic shaping :

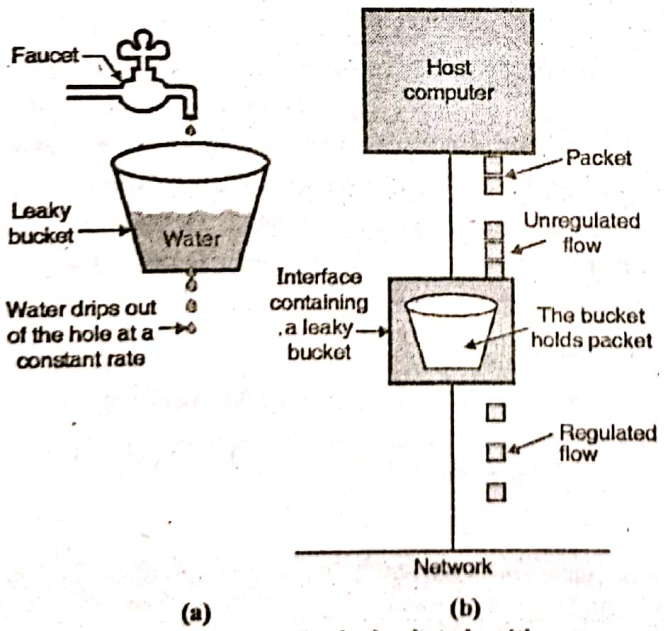
Traffic shaping is defined as a mechanism to control the amount and rate of the traffic sent to the network.

Leaky Bucket Algorithm :

Leaky bucket algorithm is used to control congestion in network traffic. As the name suggests it's working is similar to a leaky bucket in real life. The principle of leaky bucket algorithm is as follows :

Leaky bucket is a bucket with a hole at bottom. Flow of the water from bucket is at a constant rate (data rate is constant) which is independent of water entering the bucket (incoming data). If bucket is full, any additional water entering in the bucket is thrown out (Packets are discarded).

Same technique is applied to control congestion in network traffic. Every host in the network is having a buffer (equivalent to a bucket) with finite queue length. Packets which are put in the buffer when buffer is full are thrown away. The buffer may send some number of packets per unit time onto the subnet (helpful if packets vary greatly in size) as shown in Fig. 5.22 the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.

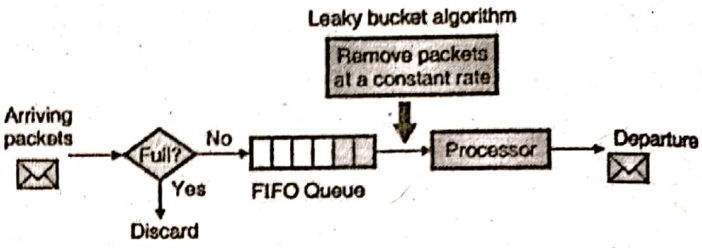


(G-481) **Fig. 5.22 : Leaky bucket algorithm**

Leaky bucket implementation :

Fig. 5.22(c) shows the implementation of leaky bucket principle. A FIFO (First In First Out) queue is used for holding the packets which is equivalent to the leaky bucket. The implementation of Fig. 5.22(c) can be under two different operating conditions, namely :

1. For packets of fixed size.
2. For packets of variable size.



(G-482) **Fig. 5.22(c) : Implementation of leaky bucket**

1. **Fixed size packets :**

   If the arriving packets are of fixed size (e.g. cells in ATM networks), then the process of Fig. 5.22(c) will allow the removal of a fixed number of packets from the queue corresponding to every tick of the clock.

2. **Packets of variable size :**

   If the packets at the input of the process are of different size, then the fixed output rate will not correspond to the number of packets leaving the process but it will correspond to the number of bits leaving the process.

Algorithm :

The algorithm for variable length packets is as follows :

1. Initialize a counter to a number "n" at the tick of the clock.
2. If "n" is greater than the packet size, then send the packet and decrement the counter by the packet size.
3. Repeat step 2 until "n" becomes smaller than the packet size.
4. Reset the counter and go back to step 1.

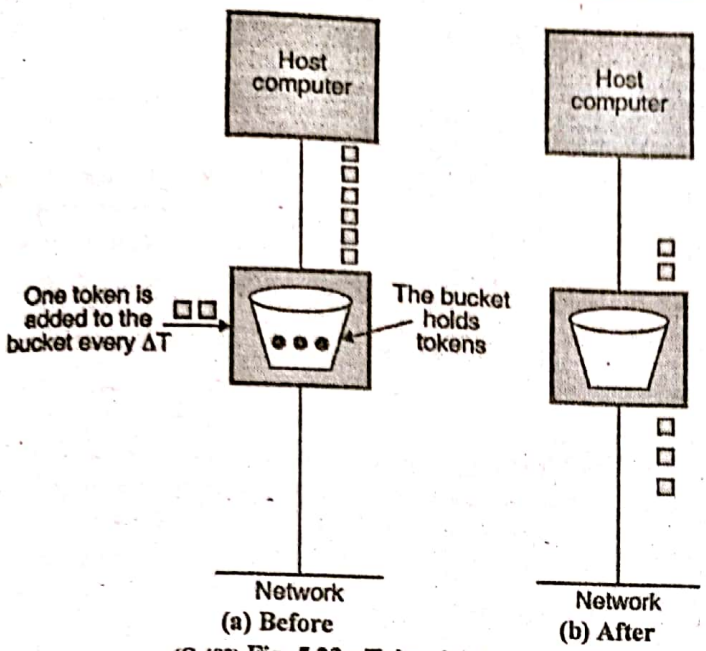
Note : Thus a leaky bucket algorithm shapes the bursty traffic to convert it into a fixed rate traffic. It does so by averaging the data rate. It drops the packets if the bucket (buffer) is full.

Q. 41 How does the token bucket algorithm works ? Dec. 10, May 15, Dec. 15, Dec. 17

Ans. :

This algorithm is similar to the leaky bucket but it is possible to vary output rates. This is useful when larger burst of traffic is received. It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to which manages the queue regulator that ultimately controls the rate of packet flow into the network. A token generator continuously produces tokens at a rate of R tokens per second and puts them into a token bucket with a depth of D tokens as shown in Fig. 5.23. If the token bucket gets full then the extra tokens are discarded.

Scanned by CamScanner



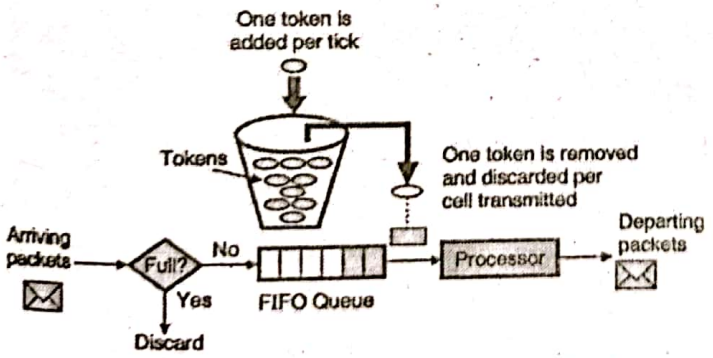
(G-483) Fig. 5.23 : Token bucket algorithm

Token bucket algorithm is a variant of leaky bucket algorithm. Here the bucket is filled with tokens.

A packet which grabs and distroies a token is allowed to leave the bucket. Due to this mechanism, the packets never get lost but they just have to wait to grab a token. At the same time, an unregulated stream of packets arrive and are placed into a packet queue that has a maximum length of L. If the flow delivers more packets than the queue can store, the excess packets are discarded.

Implementation of token bucket :

Fig. 5.23(c) shows the implementation of token bucket. The token bucket can be easily implemented with a counter. The token is initialised to zero. Every time a token is added, the counter is incremented by 1 and every time a packet is dispatched, the counter is decremented by 1. If the counter contents go to zero, the host cannot send any data.



(G-484) Fig. 5.23(c) : Implementation of token bucket

Note : The token bucket allows the bursty traffic at maximum possible rate.

Token bucket performance :

Let, s = Burst length (seconds),
c = Bucket capacity (bytes),
ρ = Token arrival rate (bytes/second),
and m = Maximum source rate (bytes/second)

What is the duration of a maximum-rate burst through a token bucket ?

1. Maximum bytes sent from the token bucket during a burst is, $c + \rho \cdot s$
2. Maximum bytes the source can send during a burst is, $m \cdot s$
3. Setting the two equal and solving for s,

$$s = \frac{c}{m - \rho}$$

Q. 42 Explain leaky bucket algorithm and compare it with token bucket algorithm. Dec. 15

Ans. :

Table 5.4 : Comparison of Token Bucket and Leaky Bucket

Sr. No.	Leaky Bucket	Token Bucket
1.	Smooth out traffic by passing packets only when there is a token. Does not permit burstiness.	Token bucket smooths traffic too but permits burstiness.
2.	Leaky bucket discards packets for which no tokens are available. (No concept of queue)	Token bucket discards token when bucket is full, but never discards packets (infinite queue)
3.	Application : Traffic shaping or traffic policing.	Application : Network traffic shaping or rate limiting

Q. 43 Explain the term: Latency. Dec. 12

Ans. :

Latency (Delay) :

The latency or delay defines how long it takes for an entire message to reach its destination from the instant at which the first bit is sent out from the source.

Latency is made of four components.

1. Processing delay
2. Queueing delay
3. Transmission delay
4. Propagation delay.

The sum of all these delays amounts to the total nodal delay.

∴ Latency = Propagation delay + Transmission delay + Queueing time + Processing delay

Q. 44 If value at HLEN field is 1101 find the size of option and padding field ? Dec. 15

Ans. :

Total length of the IP header = HLEN contents × 4 bytes
= 13 × 4 = 52 bytes.

Number of bytes corresponding to all the fields except the option + padding is 20 bytes.

∴ Size of option + padding field = 52 – 20 = 32 bytes ...Ans.

Scanned by CamScanner

Chapter 6 : Transport Layer

Q. 1 Discuss the services offered by transport layer.

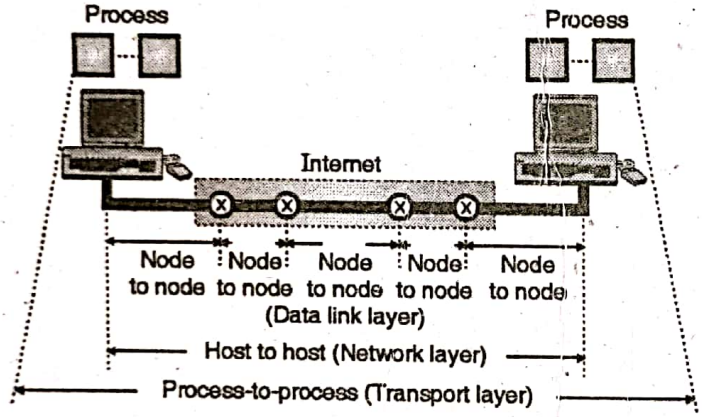
Dec. 05, May 07

Ans. :

Process-to-Process Communication :

The data link layer performs a node to node delivery. The network layer carries out the datagram delivery between two hosts (host to host delivery). But the real communication takes place between two processes or application programs for which we need the **process-to-process delivery.** The transport layer takes care of the **process-to-process delivery.** In this a packet from one process is delivered to the other process.

The relationship between the communicating processes is the client-server relationship. Fig. 6.1 demonstrates the three processes.



(G-594) **Fig. 6.1 : Types of data deliveries**

There is a difference between host-to-host communication and process to process communication that we need to understand clearly. The host to host (computer to computer) communication is handled by the network layer. But this communication only ensures that the message is delivered to the destination computer. But this is not enough.

It is necessary to handover this message to the correct process. The transport layer will take care of this.

Addressing : Port Number :

There are several ways of achieving the process-to-process communication, but the most common method is using the client-server paradigm. **Client** is defined as the process on the local host. It needs services from another process called **server** which is on the other (remote) host. Both client and server have the same name. Some of the important terms related to the client-server paradigm are :

1. Local host
2. Remote host
3. Local process
4. Remote process

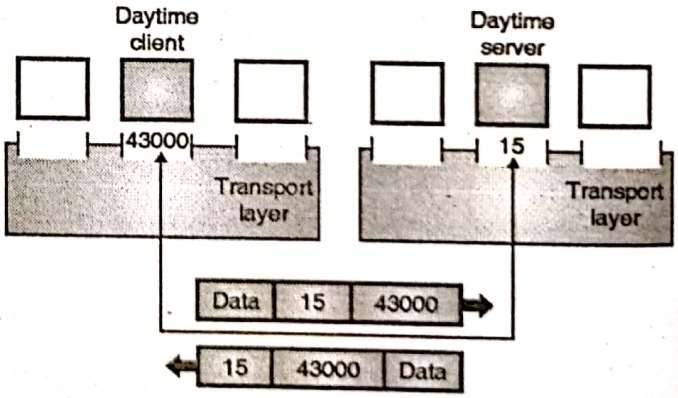
We can use the IP addresses to define the local host and remote host. But this is not enough to define a process. In order to define a process, we have to use one more identifier called **Port Numbers.** In TCP/protocol suite, the port numbers are integers and they are numbered between 0 and 65,535. At the data link layer we need a MAC address, at the network layer we need to use an IP address. A datagram uses the destination IP address to deliver the datagram and uses the source IP address for the destination's reply.

At the transport layer a transport layer addre called a **port number** is required to be used to choose among multiple processes running on the destination host. The destination port number is required to make the packet delivery and the source port number is needed to return back the reply.

In the Internet model, the port numbers are 16 bit integers. Hence the number of possible port numbers will be $2^{16} = 65,535$ and the port numbers range from 0 to 65,535.

The client program identifies itself with a port number which is chosen randomly. This number is called as **ephemeral port number.** Ephemeral means short lived. It is used because life of a client is generally short. The server process should also identify itself with a port number but this port number cannot be chosen randomly. The Internet uses universal port numbers for servers and these numbers are called as **well known port numbers.** Every client process knows the well known port numbers of the pre identified server process.

For example, a Day time client process can use an ephemeral (temporary) port number 43000 for identifying itself, the Day time server process must use the well known (permanent) port number 15. This is illustrated in Fig. 6.1(a).



(G-595) **Fig. 6.1(a) : Concept of port numbers**

Encapsulation and Decapsulation :

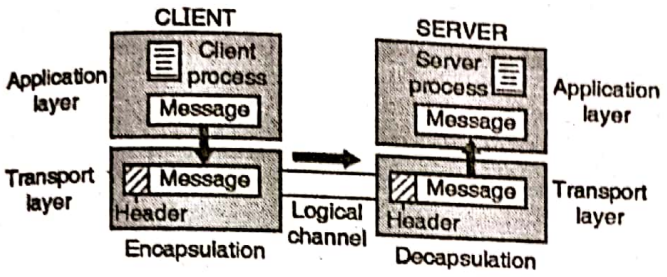
The transport layer carries out the **Encapsulation** of the message at the sending end and then **Decapsulation** at the receiving end when two computers communicate. This process has been illustrated in Fig. 6.1(b).

Encapsulation :

At the sending end the process that has a message to send, will pass it to the transport layer alongwith a pair of socket

Scanned by CamScanner

addresses and some additional information. The transport layer adds its own header to this data. This packet at the transport layer in the Internet is known by different names such as **user datagram, segment or packet.**



(G-2012) **Fig. 6.1(b) : Encapsulation and decapsulation**

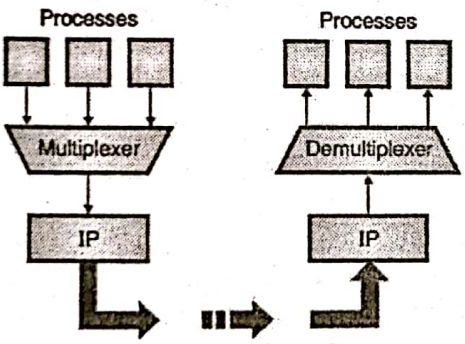
Decapsulation :

When the segment or datagram arrives at the receiving end, the header is isolated and destroyed, and the message is delivered to the process running at the application layer as shown in Fig. 6.1(b).

The socket address of the sender process is then handed over to the destination process.

Multiplexing and Demultiplexing :

The addressing mechanism allows multiplexing and demultiplexing taking place at the transport layer as shown in Fig. 6.1(c).



(G-597) **Fig. 6.1(c) : Multiplexing and demultiplexing**

Multiplexing :

At the sending end, there are several processes that are interested in sending packets. But there is only one transport layer protocol (UDP or TCP). Thus it is a many processes-one transport layer protocol situation. Such a many-to-one relationship requires multiplexing. The protocol first accepts messages from different processes. These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it. Then the transport layer adds header and passes the packet to the network layer as shown in Fig. 6.1(c).

Demultiplexing :

At the receiving end, the relationship is one as to many. So we need a demultiplexer. First the transport layer receives datagrams from the network layer.

The transport layer then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

Q. 2 Explain how TCP handles error control. Dec. 14

Ans. :

Need of error control :

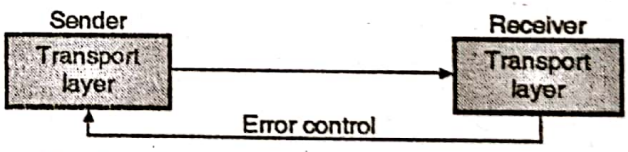
In the Internet, the network layer protocol IP has the responsibility to carry the packets from the transport layer at the sending end to the transport layer at the receiving end. But IP is unreliable. Therefore transport layer should be made reliable, in order to ensure reliability at the application layer. We can make the transport layer reliable by adding the **error control service** to the transport layer.

Duties of error control mechanism :

Following are the important responsibilities of the error control mechanism introduced at the transport layer :

1. To find and discard the corrupted packets.
2. To keep the track of lost and discarded packets and to resend them.
3. Identify the duplicate packets and discard them.
4. To buffer out of order packets until the missing packets arrive.

In the error control process, only the sending and receiving transport layers are involved. That means it is assumed that the chunk of messages exchanged between the application layers and transport layers are error free. The concept of error control at the transport layer level is demonstrated in Fig. 6.2. The receiving transport layer manages the error control by communicating with the sending transport layer about the problem.



(G-2015) **Fig. 6.2 : Concept of error control at the transport layer**

Sequence numbers :

In order to exercise the error control at the transport layer following two requirements should be satisfied :

1. The sending transport layer should know about the packet which is to be resent.
2. The receiving transport layer should know about the packets which are duplicate or the ones that have arrived out of order.

The requirements can be satisfied only if each packet has a unique **sequence number.** If a packet is either corrupted or lost the receiving transport layer will somehow inform the sending transport layer about the sequence number of those packets and request it to resend those packets. Due to the unique sequence number assigned to each packet it is possible for the receiving transport layer to identify the duplicate packets received. The out of order packets can also be recognized by observing gaps in the

Scanned by CamScanner

sequence numbers of the received packets. Packet numbers are given sequentially. But the length of the sequence number cannot be too long because the sequence number is to be included in the header of the packets.

If the header of a packet allows "m" bits per sequence number, then the range of sequence number will be from 0 to $2^m - 1$. For example if m = 3 then the range of sequence numbers will be from 0 to 7. Thus sequence numbers are modulo 2^m.

Acknowledgement :

The receiver side can send an acknowledgement (ACK) signal corresponding to each packet or each group of packets which arrived safe and sound. The question is what happens if a received packet is corrupted ? The answer is that the receiver simply discards the corrupted packet and does not send any ACK signal for it.

The sender can detect a lost packet with the help of a timer. A timer is started at the sending end as soon as a packet is sent. If the ACK does not arrive before the expiry of the timer, then the sender treats the packet to be either lost or corrupted and resends it. The receiver silently discards the duplicate packets. It will either discard the out of order packets or stored until the missing packet is received. Note that every discarded packet is treated as a lost packet by the sender.

Q. 3 Briefly explain the primary parameters that are the requirements to provide Quality of Service in networks.

Dec. 04, Dec. 06, May 09, May 15, May 16, Dec. 16

Ans. :

The QoS parameters are as follows :

1. Connection establishment delay :

The time difference between the instant at which a request for transport connection is made and the instant at which it is confirmed is called as **connection establishment delay.**

This delay should be as short as possible to ensure better service.

2. Connection establishment failure probability :

Sometimes the connection may not get established even after the maximum connection establishment delay. This can be due to network congestion, lack of table space or some other problems.

3. Throughput :

It is defined as the number of bytes of user data transferred per second, measured over some time interval. Throughput is measured separately for each direction.

4. Transit delay :

It is the time duration between a message being sent by the transport user from the source machine and its being received by the transport user at the destination machine.

5. Residual error ratio :

It measures the number of lost or garbled messages as a percentage of the total messages sent. Ideally the value of this ratio should be zero and practically it should be as small as possible.

6. Protection :

This parameter provides a way to protect the transmitted data against reading or modifying it by some unauthorised parties.

7. Priority :

Using this parameter the user can show that some of its connections are more important (have higher priority) than the other ones. This is important when congestions take place. Because the higher priority connections should get service before the low priority connections.

8. Resilience :

Due to internal problem or congestion the transport layer spontaneously terminates a connection. The resilience parameter gives the probability of such a termination.

Q. 4 What are transport service primitives ? Discuss in brief.

Dec. 15, Dec. 17

Ans. :

The transport service primitives allow the transport user such as application programs to access the transport service. Each transport service has its own access primitives. The transport service is similar to network service but there are some important differences. The main difference is that the connection-oriented transport service is reliable.

The second difference between the network service and transport service is whom the services are intended for. The transport primitives are seen by many programs and programmers. Hence the transport service is convenient and easy to use. We can get the idea about the transport services by referring to Table 6.1 which lists the five primitives.

Table 6.1 : Primitives for a simple transport service

Sr. No.	Primitive	TPDU sent	Meaning
1.	LISTEN	None	Block until some process tries to connect
2.	CONNECT	Connection request	Actively attempt to establish a connection
3.	SEND	Data	Send data
4.	RECEIVE	None	Block until a data TPDU arrives
5.	DISCONNECT	Disconnection request	Release the connection

The transport interface allows the application programs to establish, use and release connections. Now see how these primitives are used in actual applications.

Scanned by CamScanner

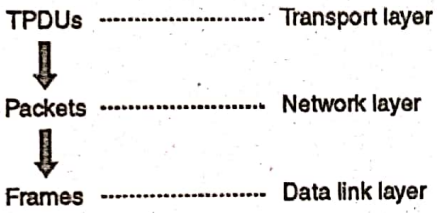
1. The server executes a LISTEN primitive. This will make a system call to block the server until a client turns up.
2. When a client wants to talk to the server it executes the CONNECT primitive.
3. In response the transport entity blocks the caller and sends a packet to the server. The transport layer message is encapsulated in the payload of this packet for the server's transport entity.

TPDU :

The message sent from transport entity to transport entity is called as transport protocol data unit or TPDU.

Nesting of TPDUs, Packets and Frames :

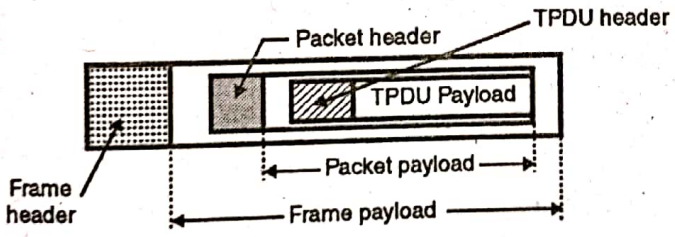
The TPDUs which are exchanged by the transport layer are contained in the packets that are exchanged by the network layer. These packets are in turn contained in the frames which are exchanged by the data link layer. When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field to the network entity.



(G-599(a)) **Fig. 6.3**

The network entity processes the packet header and passes the contents of the packet payload to the transport entity.

This is called as "Nesting" and it is illustrated in Fig. 6.3(a).



(G-600) **Fig. 6.3(a) : Nesting of TPDUs, packets and frames**

Connect primitive :

If a client gives the CONNECT call, then a connection request TPDU is sent to the server. When this TPDU arrives, the transport entity checks if the server is blocked on a LISTEN. It then unblocks the server and sends a connection accepted TPDU back to the client. On arrival of this TPDU, the client is unblocked and connection is established.

SEND and RECEIVE Primitives :

The SEND and RECEIVE primitives can be used for exchange of data. The data exchange at the network layer is more complicated than that at the transport layer. In transport layer data exchange, every data packet is eventually acknowledged. The packets carrying control TPDUs are also acknowledged.

All these acknowledgements are managed by the transport entities using the network layer protocols.

The transport entities have to take care of issues like timers and retransmission. The transport layer connection acts as a reliable bit pipe through which the bits sent by a sender come out from the other side of pipe.

Connection release :

A connection should be released when it is no longer needed. This is essential in order to free up the table space within the two transport entities. Disconnection can be of two types :

1. Asymmetric 2. Symmetric

Q. 5 Explain the term : Socket.

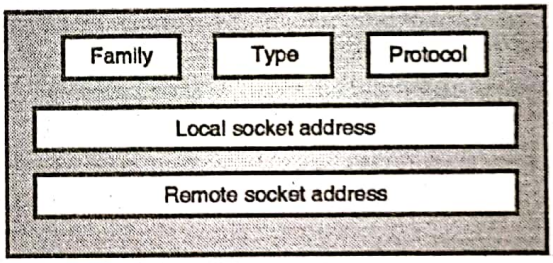
Dec. 03, Dec. 06, Dec. 07, May 08, May 09

Ans. :

The socket interface was originally based on UNIX. It defines a set of system calls or procedure. The communication structure that we need in socket programming is called as a **socket.** A socket acts as an end point. Two processes can communicate if and only if both of them have a socket at their ends.

Socket structure :

Fig. 6.4 shows a simplified socket structure.



(G-601) **Fig. 6.4 : Socket structure**

Various fields in the socket structure are as follows :

1. **Family :** This field is used for defining the protocol group such as IPv4 or IPv6, UNIX domain protocol etc.
2. **Type :** This field is used for defining the type of socket such as stream socket, packet socket or raw socket.
3. **Protocol :** This field is usually set to zero for TCP and UDP.
4. **Local socket address :** It is used for defining the local socket address. This address is a combination of local IP address and the port address of the local application program.
5. **Remote socket address :** It is used for defining the remote socket address which is a combination of remote IP address and the port address of the remote application program.

Q. 6 Write short notes on : Berkeley socket.

Dec. 09, Dec. 11, May 13, Dec. 13, May 15

Scanned by CamScanner

Ans. :

Table 6.2 lists various transport primitives used in Berkeley UNIX for TCP.

Table 6.2

Sr. No.	Primitive	Meaning
1.	SOCKET	Create a new communication end point.
2.	BIND	Provide a local address to a socket
3.	LISTEN	Show willingness to accept connections
4.	ACCEPT	Block the caller as long as a connection attempt does not arrive
5.	CONNECT	Attempt to establish a connection
6.	SEND	Send data
7.	RECEIVE	Receive data
8.	CLOSE	Release the connection

The first four primitives in the Table 6.2 are executed in the same order by the server. The SOCKET primitive creates a new end point and allocates table space for it within the transport entity.

The newly created sockets do not have addresses. These are assigned using the BIND primitive. The LISTEN primitive allocates space to queue the incoming calls in case if several clients wish to connect at the same time. To block waiting for an incoming connection, the server executes an ACCEPT primitive. When a TPDU requesting for a connection arrives, the transport entity creates a new socket and returns a file descriptor for it.

These were the primitives corresponding to server side. Now consider the client side. On the client side also a socket needs to be created first using the SOCKET primitive, however the BIND is not required. The CONNECT primitive blocks the caller and initiates the connection process. When it completes (which is indicated by an appropriate TPDU received from the server), the client process is unblocked and the connection is established.

After this both the sides can use SEND and RECEIVE primitives to send and receive data. In order to release the connection, both sides have to execute a CLOSE primitive.

Steps followed for Socket Programming :

The steps followed for the socket programming are as follows :

Server side :

1. Server creates a socket and checks for errors using SOCKET.
2. Assign address to the newly created socket using BIND.
3. Use the LISTEN to allocate space for the queue which is used for the incoming calls.
4. Execute an ACCEPT for blocking the waiting incoming connections.

Client side :

1. Create a socket using SOCKET.
2. Use CONNECT to initiate connection process.
3. Establish the connection.

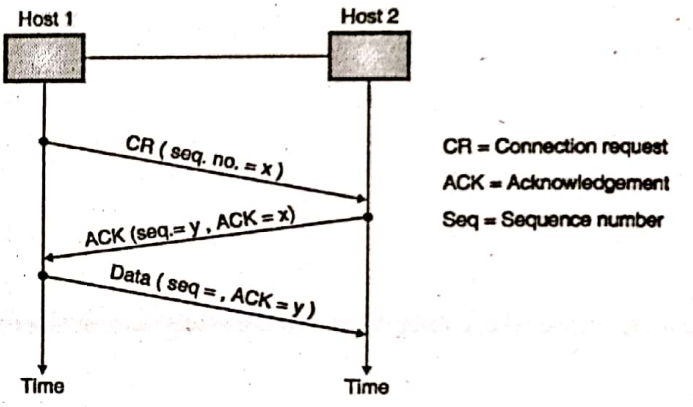
Q. 7 Explain three way handshake technique in TCP.

May 10, May 11, May 12, Dec. 13, May 15

Ans. :

The delayed duplicate packet problem can be solved by using a technique called three way handshake.

The principle of three way handshake is shown in Fig. 6.5(a).



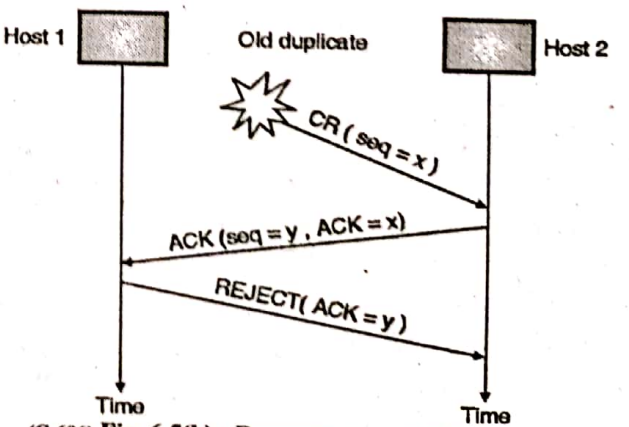
(G-605) **Fig. 6.5(a) : Three way handshake technique**

Normal operation :

1. Host 1 chooses a sequence number x and sends a TPDU containing the connection request (CR) TPDU to host 2.
2. Host 2 replies with a connection accepted TPDU to acknowledge x and to announce its own sequence number y.
3. Host 1 acknowledges host 2 and sends the first data TPDU to host 2.

Operation in the abnormal circumstances :

Now see how the three way handshake works in presence of delayed duplicate control TPDUs. Refer Fig. 6.5(b). The first TPDU is a delayed duplicate CONNECTION REQUEST from an old connection. The HOST 1 does not know about it.



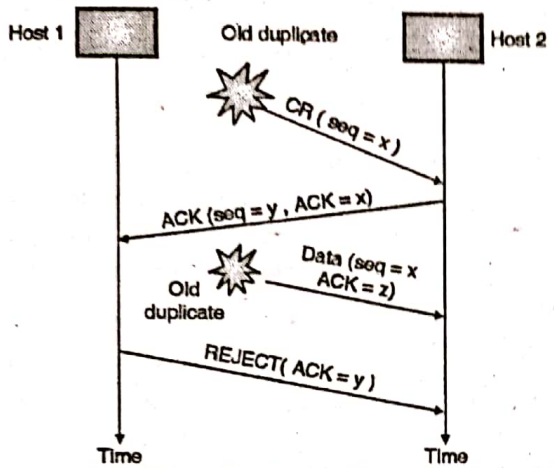
(G-606) **Fig. 6.5(b) : Response to an OLD duplicate**

Scanned by CamScanner

Host 2 receives this TPDU and sends to host 1, a connection accepted TPDU. But host 1 is not trying to establish any connection so it sends a REJECT alongwith ACK = y. So host 2 realizes that it was fooled by a delayed duplicate and abandons the connection.

Duplicate CR and duplicate ACK :

This is another abnormal situation. Refer Fig. 6.5(c) to understand this situation.



(G-607) **Fig. 6.5(c) : Duplicate CR and duplicate ACK**

This is the worst case in which delayed duplicates of both connection request (CR) and acknowledgement (ACK) are making rounds in the subnet. Host 2 gets a delayed duplicate CR and it replies to it by sending ACK. Note that host 2 has proposed a connection with a sequence number y. When the second delayed TPDU (duplicate) arrives at host 2 it understands that z has been acknowledged and not y. So it understands that this too is an OLD duplicate.

Q. 8 What is the function of TCP protocol ? Discuss its header format.

May 04, Dec. 04, May 05, May 08, Dec. 08, Dec. 10, Dec. 11

Ans. :

Take a general overview of the TCP protocol. Every byte on a TCP connection has its own 32-bit sequence number. These numbers are used for both acknowledgement and for window mechanism.

Segments :

The sending and receiving TCP entities exchange data in the form of segments. A segment consists of a fixed 20 byte header (plus and optional part) followed by zero or more data bytes.

Segment size :

The segment size is decided by the TCP software. Two limits restrict the segment size as follows :

1. Each segment including the TCP header, must fit in the 65535 byte IP payload.
2. Each segment must fit in the **MTU (Maximum Transfer Unit).** Each network has a maximum transfer unit. Practically an MTU which is a few thousand bytes defines the upper limit on the segment size.

Fragmentation :

If a segment is too large, then it should be broken into small segments. Using fragmentation by a router. Each new segment gets a new IP header. So the fragmentation by router will increase the overhead.

Timer :

The basic protocol used by TCP entities is the sliding window protocol. A sender starts a timer as soon as a sender transmits a segment. When the segment is received by the destination, it sends back acknowledgement alongwith data if any. The acknowledgement number is equal to the next sequence number it expects to receive. If the timer at the sender goes out before the acknowledgement reaches back, it will **retransmit** that segment again.

Possible problems :

As the segments can be fragmented, a part of the transmitted segment only may reach the destination with the remaining part lost. Segments can arrive out of order. Segments can get delayed so much that timer is out and unnecessary retransmission will take place. If a retransmitted segment takes a different route than the original segment is fragmented then the fragments of original and retransmitted segments can reach the destination in a sporadic way. So a careful administration is required to achieve reliable byte stream. There is a possibility of congestion or broken network along the path. TCP should be able to solve these problems in an efficient manner.

TCP Segment :

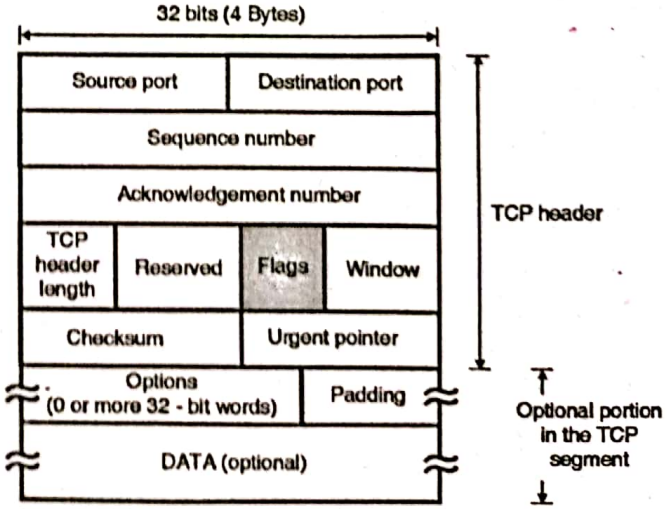
The TCP segment as shown in Fig. 6.6 consists of two parts :

1. Header
2. Data

(G-1423)**Fig. 6.6 : TCP segment**

The TCP Segment Header :

Fig. 6.6(a) shows the layout of a TCP segment. Every segment begins with a 20 byte fixed format header.



(G-611)**Fig. 6.6(a) : TCP header format**

Scanned by CamScanner

The fixed header may be followed by header options.

After the options, if any, upto 65535 – 20 – 20 = 65495 data bytes may follow. Note that the first 20 bytes correspond to the IP header and the next 20 correspond to the TCP header.

The TCP segment without data are used for sending the acknowledgements and control messages.

Source port : A 16-bit number identifying the application the TCP segment originated from within the sending host. The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49,151) and private ports (49,152 through 65,535). Port assignments are used by TCP as an interface to the application layer.

Destination port : A 16-bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports.

Sequence number : A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection. After reaching $2^{32} - 1$, this number will wrap around to 0.

Acknowledgement number :

A 32-bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on.

Header length or offset :

A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer). Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes. This field is required because the size of the options field(s) cannot be determined in advance. Note that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

Reserved :

A 6-bit field currently unused and reserved for future use.

Control bits or flags :

1. **Urgent pointer (URG) :** If this bit field is set, the receiving TCP should interpret the urgent pointer field.
2. **Acknowledgement (ACK) :** If this bit field is set, the acknowledgement field described is valid.
3. **Push function (PSH) :** If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible. An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.
4. **Reset the connection (RST) :** If this bit is present, it signals the receiver that the sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinquished.
5. **Synchronize (SYN) :** When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.
6. **No more data from sender (FIN) :** If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window :

A 16-bit integer used by TCP for flow control in the form of a data transmission window size. This number tells the sender how much data the receiver is willing to accept. The maximum value for this field would limit the window size to 65,535 bytes, however a "window scale" option can be used to make use of even larger windows.

Checksum : A TCP sender computes a value based on the contents of the TCP header and data fields. This 16-bit value will be compared with the value the receiver generates using the same computation. If the values match, the receiver can be very confident that the segment arrived intact.

Urgent pointer :

In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible. This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options :

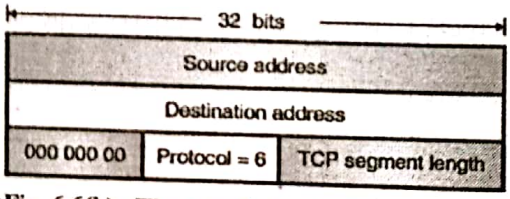
In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver. Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits). The most common option is the Maximum Segment Size (MSS) option. A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option. Other options are often used for various flow control and congestion control techniques.

Padding :

Because options may vary in size, it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32-bit word boundary as defined by the standard.

Data :

Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header fields constitutes a TCP segment. A checksum is provided to ensure extreme reliability. It checksums the header, the data and the conceptual pseudo header shown in Fig. 6.6(b).



(G-612)**Fig. 6.6(b) : The pseudo header included in the TCP checksum**

Scanned by CamScanner

When the checksum is being computed, the TCP checksum field is set to zero, and the data field is padded out with an additional zero byte if its length is an odd number.

Then all the 16 bit words are added in 1's complement and then 1's complement of the sum is taken to get the checksum.

When a receiver performs the calculation on the entire segment including the checksum field, the result has to be zero.

The pseudo header contains the 32 bit IP address of the source and destination machines, the protocol number for TCP i.e. 6 and the TCP segment length as shown in Fig. 6.6(b).

Q. 9 Show how TCP connection setup protects against the situation in :

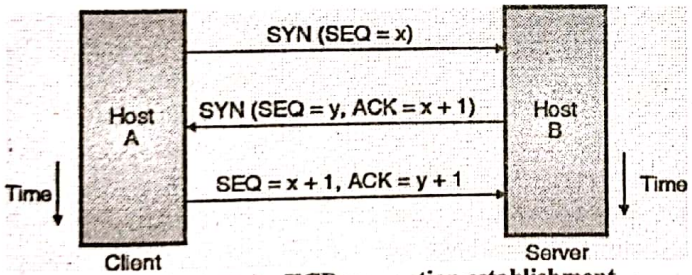
Draw the space time diagram for protocol message exchange and explain how the protocol works. Dec. 03

Ans. :

TCP Connection Establishment :

To make the transport services reliable, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a **three-way handshake** mechanism. A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well.

This is necessary so that packets are not transmitted or re-transmitted during session establishment or after session termination. Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the manner shown in Fig. 6.7(a).



(G-613) **Fig. 6.7(a) : TCP connection establishment (Three-way handshake)**

The requesting end (HOST A) sends a SYN segment specifying the port number of the server that the client wants to get connected to, and the client's initial sequence number (x). The server (HOST B) responds with its own SYN segment containing the server's initial sequence number (y). The server also acknowledges the client's SYN by acknowledging the client's SYN plus one (x + 1). A SYN consumes one sequence number.

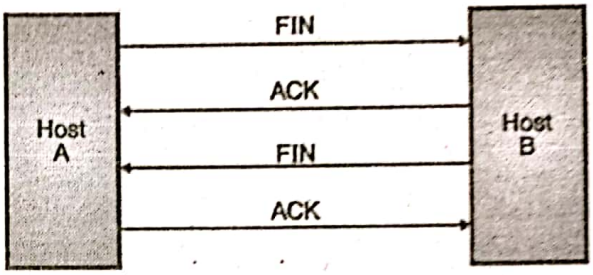
The client must acknowledge this SYN from the server by acknowledging the server's SYN plus one. (SEQ. = x + 1, ACK = y + 1). This is how a TCP connection is established.

Connection Termination Protocol [Connection Release] :

While it takes three segments to establish a connection, it takes four to terminate a connection. Since a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), the connection should be terminated in both the directions independently.

The termination procedure in each direction is shown in Fig. 6.7(b). The rule is that either side can send a FIN when it has finished sending data (FIN indicates finished).

When a TCP program on a host receives a FIN, it informs the application that the other end has terminated the data flow.



(G-614) **Fig. 6.7(b) : TCP termination**

The receipt of a FIN only means there will be no more data flowing in that direction. A TCP can still send data after receiving a FIN. The end that first issues the close (e.g., sends the first FIN) performs the active close and the other end (that receives this FIN) performs the passive close. Now refer Fig. 6.7(b). When the server receives the FIN it sends back an ACK of the received sequence number plus one. A FIN consumes a sequence number, just like a SYN. At this point the server's TCP also delivers an end-of-file to the application (the discard server).

The server then closes its connection and its TCP sends a FIN to the client. The client's TCP informs the application and sends an ACK to server by incrementing the received sequence number by one. Connections are normally initiated by the client, with the first SYN going from the client to the server. A client or server can actively close the connection (i.e. send the first FIN). But in practice generally the client determines when the connection should be terminated, since client processes are often driven by an interactive user, who enters something like quit to terminate.

This is how the TCP connection is released.

Q. 10 Explain with the help of suitable diagram TCP connection management and release.

Dec. 03, Dec. 15, May 17, Dec. 17

Ans. :

TCP Connection Management :

Connections are established in TCP by following the three-way handshake technique. To establish a connection, one side, say the server, passively waits. It executes the LISTEN and ACCEPT primitives, to specify either a particular other side or nobody in particular. The other side (client) executes a connect primitive, with the IP and the port specified.

The other information is the maximum TCP segment size, possible other options and optionally some user data (e.g. a password).

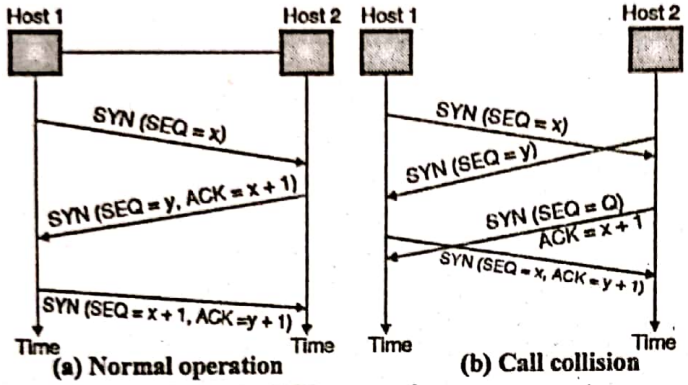
The CONNECT primitive sends a TCP segment with the SYN bit on and the ACK bit off and waits for a response. The sequence of TCP segments sent in the normal case is shown in Fig. 6.8(a).

When the segment sent by Host –1 reaches the destination i.e. host – 2 the receiving server checks to see if there is a process that

Scanned by CamScanner

has done a LISTEN on the port given in the destination port field. If not, it sends a reply with the RST bit on to reject the connection.

Otherwise it gives the TCP segment to the listening process, which can accept or refuse (e.g. if it does not like the client) the connection. On acceptance a SYN is send, otherwise a RST. Note that a SYN segment occupies 1 byte of sequence space so it can be acknowledged unambiguously.



(a) Normal operation (b) Call collision

(G-615) Fig. 6.8 : TCP connection management

Call collision :

If two hosts try to establish a connection simultaneously between the same two sockets then the events take place as shown in Fig. 6.8(b). Under such circumstances only one connection is established. Both the connections can not be established simultaneously because connections are identified by their end points. If the first set up results in a connection which is identified by (x, y) and second connection is also set up, then only one table entry will be made i.e. for (x, y).

For the initial sequence number a clock based scheme is used, with a clock pulse coming after every 4 μsec. For ensuring an additional safety, when a host crashes, it may not reboot for 120 sec which is maximum packet lifetime. This is to make sure that no packets from previous connections are still alive and travelling around.

TCP Connection Release :

A TCP connection is actually a full duplex connection but to understand the connection release we will assume that it is a pair of simplex connections. We can then think that each simplex connection is getting terminated independently.

Releasing a TCP connection is identical on both ends. Each side can send a TCP segment with the FIN bit set, meaning it has no more data to send. After receiving a FIN, the Acknowledge (ACK) signal is sent and that direction is shut down, but data may continue to flow indefinitely in the other direction.

If the sender of FIN does not receive the ACK within 2 maximum packet lifetimes, it releases the connection. The receiver will eventually notice that it receives no more data and time-out as well. Normally four TCP segments are required to release a connection i.e. one FIN and one ACK in each direction.

However the first ACK and second FIN can be combined in the same segment.

Connection reset :

The connection reset in TCP can take place when TCP at one end done any one of the following :

1. It may deny a connection request.
2. It may abort the existing connection.
3. It may terminate an idle i.e. non operating connection.

TCP does all the three with the help of the RST (reset flag).

Q. 11 Discuss the window management in TCP transmission policy with a neat diagram. Dec. 10

Ans. :

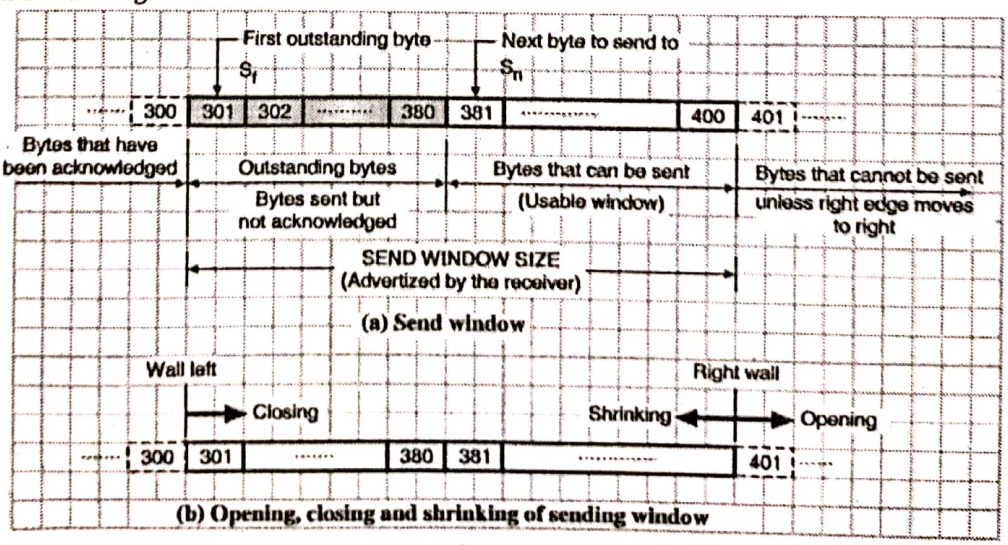
Here we will see the windows used in TCP. There are two types of windows used in TCP :

1. Send window 2. Receive window

Send window is for sending data and receive window is for receiving data. Therefore there will be four windows in all for a two way communication. However in order to make simple, we will assume that the communication takes place only in one direction (client to server or the other way round).

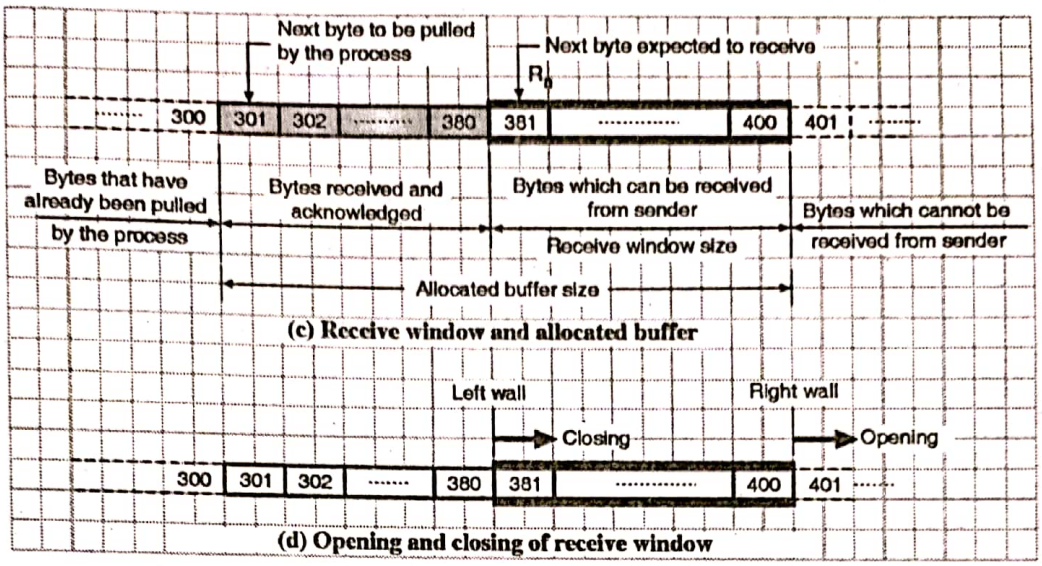
Send Window :

Fig. 6.9 illustrates an example of send window. In reality the send window can have a size of thousands of bytes for a 100 byte send window has been considered in Fig. 6.9.



(G-1800) Fig. 6.9 : Send window in TCP

Scanned by CamScanner



(G-1801) **Fig. 6.9 : Receive window in TCP**

The size of send window is dependent on the receiver (flow control) as well as on the congestion control. There are three operations that can take place in the send window, namely : open, close and shrink. The send window in TCP is similar to that in selective repeat request (SR) with the following differences :

1. The SR send window numbers pockets but TCP send window numbers bytes. In TCP the transmission takes place in the form of segments but the controlling parameters of windows are expressed in bytes.
2. Actually TCP is capable of storing data received from the process and send it later on. But we will assume that the sending TCP sends the segments of data as soon as it is received from the process.
3. TCP uses only one timer as compared to several timers used by the SR protocol. This timer in TCP is used for error control.

Receive Window :

The example of receive window has been shown in Fig. 6.9. In reality the receive window can have size of thousands of bytes a 100 byte receive window has been shown in Fig. 6.9.

The receive window in TCP is similar to that in selective repeat request (SR) with the following differences :

1. The receiving process in TCP is allowed to pull data as per its own speed. That means in a part of allocated buffer there are bytes which have been received and acknowledged but waiting for the receiving process to pull them (see Fig. 6.9). The size of receive window is therefore always smaller than the allotted buffer size. The size of the receive window will decide the number of bytes a receiver can receive without causing the flow control problems. The receiver window size which is denoted by "rwnd" is expressed as follows :

rwnd = Buffer size – Number of acknowledged bytes to be pulled

2. The acknowledgements in SR define the uncorrupted received packets only. This is selective acknowledgement. However in TCP the mechanism of acknowledgement is called as **cumulative acknowledgement** in which the next expected byte to be received (R_n = 381 in Fig. 6.9) is announced. The new version of TCP uses both selective and cumulative mechanisms for acknowledgements.

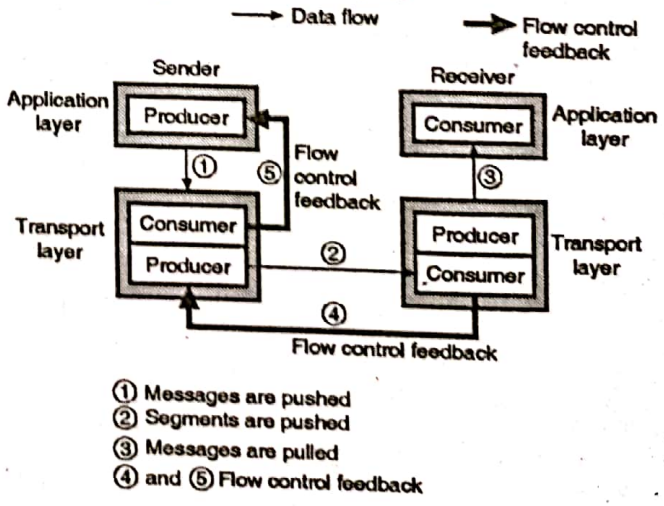
Q. 12 Explain how TCP handles flow control. Dec. 14

Ans. :

The flow control is a technique used for controlling the data rate of the sender so that the receiver is not overwhelmed.

In TCP the flow control has been kept separate from the error control. So when the flow control is being seen, we will temporarily ignore the error control. i.e. we assume that the data transmission is taking place over an error free channel.

Refer Fig. 6.10 which shows the data transfer taking place in only one direction from the sender to receiver. We can apply the same principle to the bidirectional data transfer. Two different types of signals travel between the sending process and the receiving process in Fig. 6.10. They are data and flow control feedback signals. The data flow takes place from the sending process to the sending TCP (denoted by ①), then from sending TCP to receiving TCP (denoted by ②) and finally from receiving TCP to receiving process (denoted by ③).



(G-1802) **Fig. 6.10 : Data flow and flow control feedback in TCP**

Scanned by CamScanner

Thus flow of data takes place from sender to receiver. But the flow control feedback signals travel from the receiver to sender as shown. They flow from receiving TCP to sender TCP (denoted by ④) and from sending TCP to sending process (denoted by ⑤). Most TCP versions however, do not provide the flow control feedback facility. Instead the receiving process is allowed to pull data from receiving TCP whenever the receiving process becomes ready. Thus the receiving TCP controls the sending TCP (due to flow control feedback) and the sending TCP controls the sending process as far as the data rate of the sending process is concerned.

Consider the flow control feedback path denoted by ⑤ in Fig. 6.10. This feedback is practically achieved by simply rejecting the data by sending TCP when its window is full. So now concentrate on the flow control feedback signal from receiving TCP to sending TCP, denoted by path ④ in Fig. 6.10. i.e. how does the receiving process control the sending TCP.

Q. 13 Explain how TCP controls congestion.

May 07, Dec. 07, May 08, May 09, Dec. 09, May 13, Dec. 14

Ans. :

The network layers detects the congestion by looking at the growing queues at the routers and tries to manage it by dropping packets. The network layer has to give feedback to the transport layer about the possible congestion because only then the transport layer can reduce the sender's data rate.

In the Internet, TCP plays a major role in controlling congestion. A control law called AIMD (Additive Increase Multiplicative Decrease) can be used in response to binary congestion signals received from the network. According to this law, in response to congestion signals the transport protocol should converge to a fair and efficient bandwidth allocation. TCP congestion control is based on this approach using a **window** and with a loss of packet used as the binary signal to indicate congestion.

Principle of congestion control :

The basic principle is do not inject a new packet into the network until an old one is delivered. TCP tries to do this by dynamically adjusting the window size. The steps followed in achieving the congestion control in TCP are as follows :

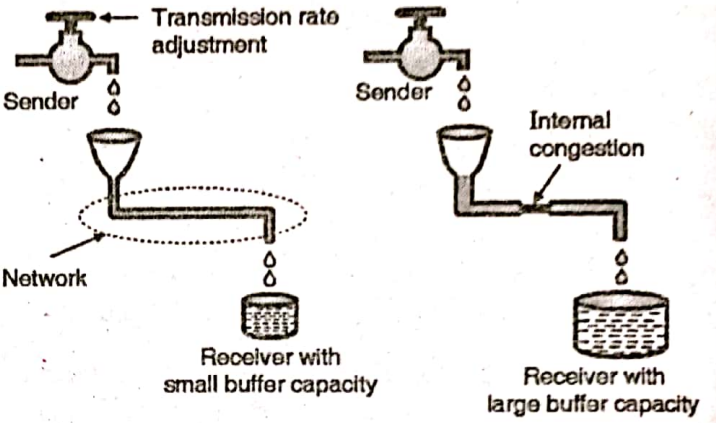
Step 1 : Detect the congestion :

This is the first step in congestion control. Now-a-days packet loss due to transmission errors is very rare because the optical fiber links are being used. So most transmission time-outs (loss of packets) are due to congestions. So all the Internet TCP algorithms assume that time-outs are caused by congestion and so time outs can be used to detect the congestion.

Step 2 : Try to prevent congestion :

After establishing a connection, a suitable window size is to be chosen. The receiver window size is based on its buffer capacity. If the sender adjusts its transmission rate according to this capacity as shown in Fig. 6.11(a), the congestion due to buffer overflow will never take place. Now consider Fig. 6.11(b). The sender is slow, the receiver has a large buffer capacity but the problem is low internal carrying capacity of the network.

If the sender is too fast, the water will back up and some will be lost (loss of packets) and congestion will take place.



(a) No congestion (b) Internal

(G-618) **Fig. 6.11 : Congestion**

Conclusion :

To prevent congestion TCP has to deal with two problems separately – receiver capacity and network capacity.

Solution :

To deal with the two problems mentioned, each sender maintains two windows : the window the receiver has granted (which indicates the receiver capacity) and the **congestion window** (which indicates the network capacity). The first window that indicates the receiver capacity is called as the **flow control window.** The size of the congestion window is equal to the number of bytes the sender may have in the network at any time. Hence the corresponding **sending rate** is equal to the ratio of **congestion window size** and the **RTT** of the connection. TCP adjusts the size of window as per the AIMD rule.

The **congestion window** is maintained in addition to the **flow control window** (Which specifies the number of bytes that the receiver can buffer). Both these windows are considered simultaneously. Both the windows indicate the number of bytes the sender may transmit and the number can be different. Therefore the number of bytes that may be sent by the sender is the minimum of the two windows. So the effective window is the minimum of what the sender and the receiver both think is all right.

Modern congestion control :

Modern congestion control was added to TCP in 1988 through the efforts of Van Jacobson. In 1986 due to growing number of Internet users the first **congestion collapse** took place. As a response to this collapse Jacobson approximated an AMID congestion window and added it to the existing TCP. While doing so he made following two important considerations :

1. The rate at which the acknowledgements return to the sender is approximately equal to the rate at which packets can be sent over the slowest link in the path. This is the rate a sender

Scanned by CamScanner

wants to use to avoid congestion. This timing is known as **ACK clock** and it is an essential part of TCP. Using ACK clock TCP smoothes out traffic and avoids congestion.

2. The second consideration was that AMID rule will take a very long time to reach the desired operating point on fast networks if the congestion window is started from a small value. The start up time can be reduced by using a large initial window. But a too large starting window would cause congestion in slow or short links.

Hence Jacobson mixed both linear and multiplicative increase in the window size in his solution to resolve congestion. This modified algorithm is known as the **slow start** algorithm.

Q. 14 Differentiate between TCP and UDP.

Dec. 04, Dec. 05, Dec. 07, May 11

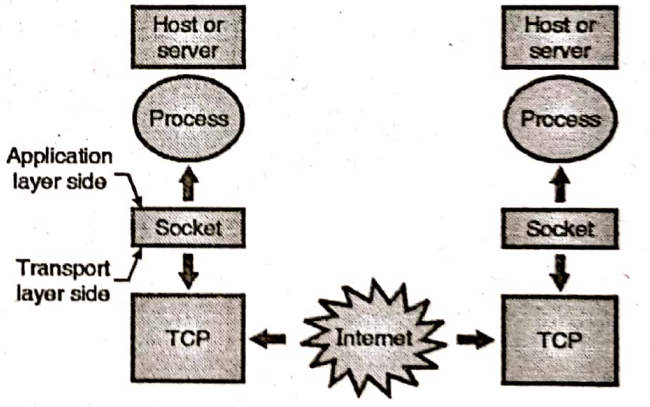
Ans. :

Characteristic / Description	UDP	TCP
General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quantity	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols.
Well-Known Applications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions).	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions).
Error control	Only checksum.	Provided.

Q. 15 Write a program for client-server application using socket programming (TCP).

May 16, Dec. 17

Ans.: The processes running on different machines communicate with each other by sending messages into sockets. This is demonstrated in Fig. 6.12.

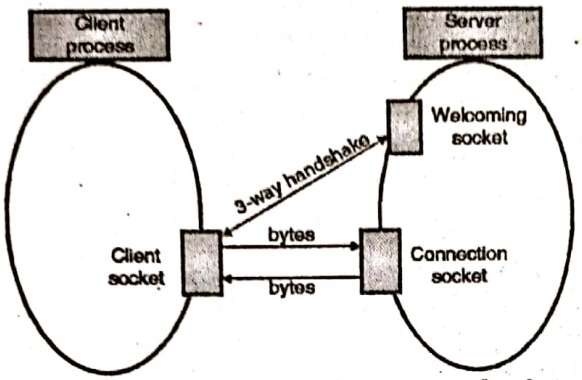


(G-630) **Fig. 6.12 : Communicate between processes through TCP sockets**

Socket acts as a door between the application process and TCP as shown in Fig. 6.12. The application developer controls everything on the application layer side of the socket but does not have any control over the transport layer side of the socket. The interaction of the client and server takes place as follows. The client has to initiate contact with the server and when such a contact is being initiated, the server should be ready. That means the server must be a running process (not dormant) when a client initiates contact and the server process must have a socket to welcome the initial contact from the client. With the server process

Scanned by CamScanner

running, the client process can initiate a TCP connection to the server. This is done in the client program by creating a socket. When the client socket is created, the client specifies the address of the server process i.e. the IP address of the server process i.e. the IP address of the server host and the port number of the server process.



(G-1247) **Fig. 6.12(a) : Different types of sockets**

Then the TCP on the client side initiates a three way handshake and establishes a connection with the server. The three way handshake and the TCP connection establishment is shown in Fig. 6.12(a). During the three way handshake the client process knocks on the welcoming socket of the server process. The server process responds to this knocking by creating a new socket called **connection socket** which is dedicated to that particular client. In the last phase of the three way handshake a TCP connection is established between the client socket and the connection socket as shown in Fig. 6.12(a). The TCP connection is equivalent to a direct virtual pipe between the clients socket and server's connection socket to allow a reliable byte-stream service between the client process and server process.

Q. 16 Write a program for client-server application using Socket Programming (UDP). Dec. 16

Ans. :

When two processes communicate over a TCP connection, it is equivalent to communicating over a virtual pipe between the two processes. This pipe will remain in place until one of the processes terminates the TCP connection. The sending process does not have to insert the destination address to the bytes to be sent because the virtual connection is existing. Also the pipe provides a reliable byte transfer without altering the sequence in which the bytes are received. Like TCP, the UDP also allows two or more processes running on different hosts to communicate. But there is a major difference.

The first difference is that UDP provides a connectionless service so there is no handshaking process in order to establish the virtual pipe like TCP. As there is no virtual pipe existing, when a process wants to send a batch of bytes to the other process, the sending process has to attach the address of the destination process. The destination address is a tuple consisting of the IP address of the destination host and the port number of the destination process. The IP address and port number together are called as **"packet".**

UDP provides an unreliable message oriented service in which there is no guarantee that the bytes sent by the sending process will reach the destination process. After creating a "packet", the sending process will push the packet into the network through a socket. This packet is then driven in the direction of destination process. The code for UDP socket programming is different than that for TCP in the following ways :

1. No need for a welcoming socket as no handshaking is needed.
2. No streams are attached to the socket.
3. The sending host has to create packets.
4. The receiving process has to obtain information from each received packet.

Chapter 7 : Application Layer

Q. 1 Write a short notes on : DNS. Dec. 14, May 15, Dec. 17

Ans. : Addressing :

For communication to take place successfully, the sender and receiver both should have addresses and they should be known to each other. The addressing in application program is different from that in the other layers. Each program will have its own address format. For example an e-mail address is like sachinshaha@vsnl.net where as the address to access a web page is like http :// www.google.com/ It is important to note that there is an alias name for the address of remote host. The application program uses an alias name instead of an IP address. This type of address is very convenient for the human beings to remember and use. But it is not suitable for the IP protocol. So the alias address has to be mapped to the IP address. For this an application program needs service of another entity.

This entity is an application program called DNS. Note that DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

How does DNS Work ?

To map a name onto an IP address, an application program calls a library procedure called the **resolver.** The name is passed on to the resolver as a parameter. The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver. The resolver then sends this address to the caller. Then the program can establish a TCP connection with the destination or sends in the UDP packets.

Q. 2 Give short notes on : HTTP. Dec. 14

Ans. :

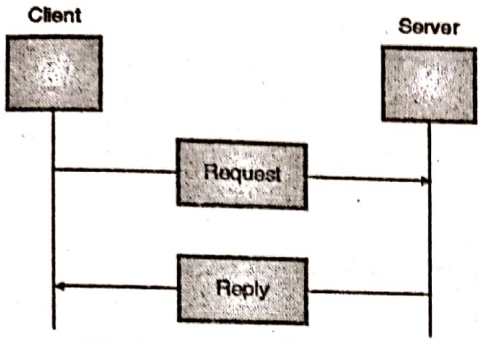
The main function of HTTP is to access data on WWW. This protocol can access the data in various forms such as plaintext, hypertext, audio, video etc.,

The function of HTTP is equivalent to a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection (port 80). There is no separate control connection like the one in FTP. Only the data transfer takes place between the client and server so there is only one connection and it is the data connection. The data transfer in HTTP is similar to SMTP. The format of the messages is controlled by MIME like headers.

Principle of HTTP Operation :

The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format. Fig. 7.1 shows the HTTP transactions between client and server. The client initializes the transaction by sending a request message and the server responds by sending a response.

Scanned by CamScanner



(G-657) Fig. 7.1 : HTTP transaction

Non-persistent and Persistent Connection :

HTTP is capable of using both non-persistent and persistent connections. HTTP uses persistent connection in its default mode. But HTTP clients and servers can be configured to use the non-persistent connection as well.

1. Non-persistent connections :

Now see the step-by-step procedure followed for transferring a web page from server to client for a non-persistent connection. Imagine that the web page consists of a base HTML file and many JPEG images and that all these objects reside on the same server. Let the URL for the base HTML file be as follows :

http://www.vit.edu/itdept/home.index

Then the sequence of events is as follows :

1. The HTTP client process initiates a TCP connection to the server www.vit.edu on port number 80, which is the default port number for HTTP.
2. The HTTP client, sends an HTTP request message to the server via its socket associated with the TCP connection. This request message is of the following format :

   Path name/itdept/home.index.
3. The HTTP server process receives the request message via its socket associated with the connection. It then retrieves the object.

   /itdept/home.index

   from its storage. It then encapsulates this retrieved object in an HTTP response message and sends the response message to the client via its socket.
4. The HTTP server process tells TCP to close the TCP connection.
5. As soon as the HTTP client receives the response message, the TCP connection is terminated.
6. The response message indicates that the encapsulated object is an HTML file. The client takes out the file from the response message and examines the HTML file. The client will find references to all the JPEG objects.
7. The client follows the first four steps for each JPEG object.

As the browser receives the web page, it displays the page. Different browsers can display the same web page differently. However HTTP is not concerned about this. Its specifications define only the communication between the HTTP client program and HTTP server program. In **non-persistent** connection where each TCP connection is closed after the server sends the object. That means the TCP connection does not persist for other objects. Each TCP connection transports one request message and one response message.

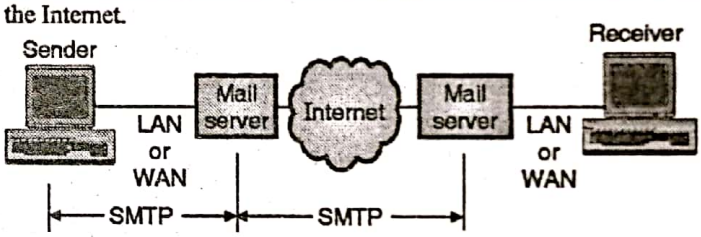
2. Persistent connection :

The disadvantages of non-persistent connections can be overcome if persistent connection is used. With the persistent connection, the server leaves the TCP connection open after sending a response. All the requests and responses between the same client and server can be sent over the same connection. Hence the entire web page can be sent over a single persistent connection. It is also possible to send the multiple web pages reciding on the same server to the same client over a single persistent TCP connection. The TCP connection is closed only after the time out interval by the HTTP server.

Q. 3 Write short notes on : SMTP. Dec. 16, Dec. 17

Ans. :

The actual mail transfer is carried out through the message transfer agent. A system should have the client MTA in order to send a mail and it should have a server MTA in order to receive one. SMTP is the protocol which defines MTA client and server in the Internet.



(G-641)Fig. 7.2 : SMTP range

As shown in Fig. 7.2, the SMTP is used twice, once between the sender and sender's mail server and then between the two mail servers. The job of SMTP is simply to define how commands and responses be sent back and forth. Each network can choose its software package for implementation.

SMTP (Simple Mail Transfer Protocol) :

In Internet the source machine establishes a connection to port 25 of the destination machine so as to deliver an e-mail. An e-mail daemon which speaks SMTP is listening to this port. This daemon is supposed to perform the following tasks :

1. Accept the incoming connections, and copy messages from them into appropriate mailboxes.
2. Return an error message to the sender, if a message is not delivered.

SMTP is a simple ASCII protocol.

Once a TCP connection between a sender and port 25 of the receiver is established, the sending machine operates as a client and the receiving machine acts as a server. The client then waits for the server to take initiative in communication. The server sends a line of text which decares its identity and announces its willingness/ unwillingness to receive mail. If the server is not prepared, the client will release the connection, wait for sometime and try again later.

But if the server is willing to accept e-mail, then the client announces the sender of e-mail and its recipient. If such a recipient exists at the destination, then the server tells the client to send the message. The client, then sends the message and the server sends back its acknowledgement. No checksums are generally required because TCP provides a reliable byte stream. If there are any more

Scanned by CamScanner

e-mail, then they can be sent now. After exchanging all the e-mail, the connection is released. SMTP uses numerical codes. The lines sent by the client are marked C : ; and those sent by the server are marked S : ;

Some of the commands, useful for communication are :

HELO, RCTP, DATA, QUIT etc.

RCTP represents recipient. If only one command is used then the message is being sent to only one recipient. If the command is used many times, then it indicates that the message is sent to more than one recipients. In such a case each message is individually acknowledged or rejected. The syntax of four character commands for the clients are rigidly specified but the syntax for the replies are not that rigid. The SMTP protocol is well defined by RFC 821 but some problems are still present.

Problems in SMTP :

Some of the problems in SMTP are as follows :

1. Some older versions of SMTP are not capable of handling messages longer than 64 kB.
2. If client and server have different time-outs, then one of them may give up when the other is still busy. This will terminate the connection unnecessarily.
3. In rate situations, infinite mailstorms can be triggered.

Extended SMTP (ESMTP) :

Some of these problems can be solved by using the extended SMTP (ESMTP) which is defined in RFC 1425.

□□□

Scanned by CamScanner

Computer Networks (MU)

Statistical Analysis

Chapter No.	Dec. 2018	May 2019
Chapter 1	18 Marks	15 Marks
Chapter 2	04 Marks	10 Marks
Chapter 3	14 Marks	15 Marks
Chapter 4	20 Marks	45 Marks
Chapter 5	68 Marks	20 Marks
Chapter 6	10 Marks	15 Marks
Chapter 7	10 Marks	10 Marks
Repeated Questions	–	51 Marks

Dec. 2018

Chapter 1 : Introduction to Networking [Total Marks - 18]

Q. 1(a) What are the design issues for the OSI layers ? (4 Marks)

Ans. :

Design issues for the OSI layers :

Addressing :

- For every layer, it is necessary to identify senders and receivers. Some mechanism needs to be used for the same.
- Since there are many possible destinations for a packet, some form of addressing is needed in order to specify a specific destination.

Error control :

- Another important issue is the error control because physical communication channels can introduce errors in the data travelling on them.
- Error detection and correction both are essential.
- Many error detecting and correcting codes are known out of which those which are agreed upon and receiver should be used.
- The receiver should be able to tell the sender by some means, that it has received a correct message or a wrong message.

Avoid loss of sequencing :

- All the communication channels cannot preserve the order in which messages are sent on it.
- So there is a possibility of loss of sequencing. That means messages are not received serially at the receiver.
- To avoid this, all the packets of a message should be numbered so that they can be put back together at the receiver in the appropriate sequence.

Ability of receiving long messages :

- At several levels, one more problem needs to be solved, which is inability of all processes to accept arbitrarily long messages.
- So a mechanism needs to be developed to deassemble (break into small messages), transmit and then reassemble messages.

To use multiplexing and demultiplexing :

- Multiplexing and demultiplexing is to be used to share the same channel by many sources simultaneously.
- It can be used for any layer. Multiplexing is needed at the physical layer level.

Q. 1 (b) Differentiate between connection oriented and connectionless service ? (4 Marks)

Ans. :

Comparison of connection oriented and connectionless services :

Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection needs to be established	Connection need not be established
6.	Delays	More	Less

Scanned by CamScanner

Sr. No.	Parameter	Connection oriented	Connectionless
7.	Overheads	Less	More
8.	Packets travel	Sequentially	Randomly
9.	Congestion due to overloading	Not possible	Very much possible

Q. 2(a) What is topology ? Explain the types of topologies with diagram, advantages and disadvantages. (10 Marks)

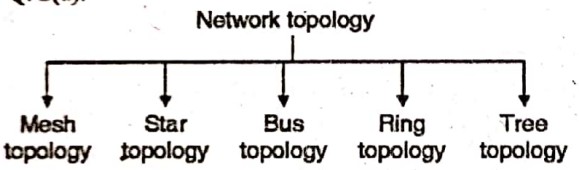
Ans. :

Topology :

Topology is the word used to explain the manner in which a network is physically connected. Devices or nodes in a network get connected to each other via communication links and all these links are related to each other in one way or the other.

Types of topologies :

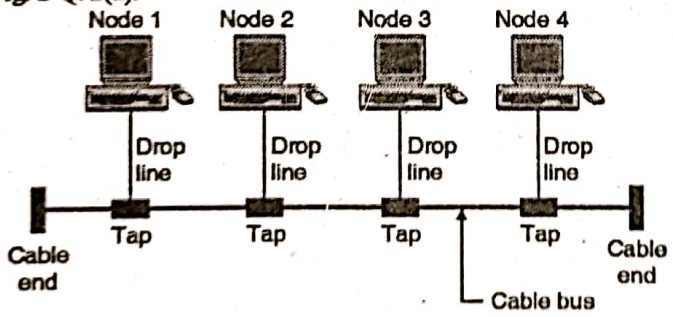
The five basic network topologies are as shown in Fig. 1-Q. 2(a).



(G-14) **Fig. 1-Q. 2(a) : Classification of network topology**

1. Bus topology :

The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 2-Q. 2(a).



(G-15) **Fig. 2-Q. 2(a) : Bus topology**

- On a typical bus network a simple cable is used without additional electronics to amplify the signal or pass it along from computer to computer. Therefore the bus is a passive topology.
- The bus topology requires a proper termination at both the ends of the cable in order to avoid reflections.
- Since the bus is a passive topology, the electrical signal from a transmitting computer is free to travel over the entire length of the cable. Thus addition and cancellation of wave results in a standing wave.

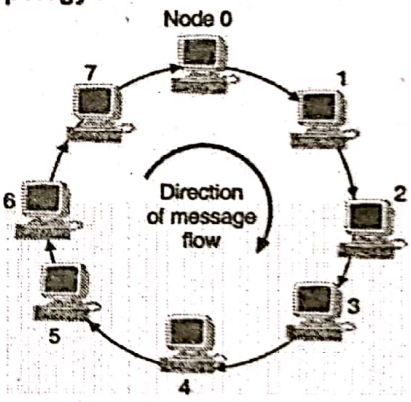
Advantages of bus topology :

1. The bus topology is easy to understand, install, and use for small networks.
2. The cabling cost is less as the bus topology requires a small length of cable to connect the computers.
3. The bus topology is easy to expand by joining two cables with a BNC barrel connector.
4. In the expansion of a bus topology repeaters can be used to boost the signal and increase the distance.

Disadvantages of bus topology :

1. Heavy network traffic slows down the bus speed. In bus topology only one computer can transmit and other have to wait till their turn comes and there is no co-ordination between computers for reservation of transmitting time slot.
2. The BNC connectors used for expansion of the bus attenuates the signal considerably.
3. A cable break or loose BNC connector will cause reflections and bring down the whole network causing all network activity to stop.

2. Ring topology :



(G-16) **Fig. 3-Q. 2(a) : Ring topology**

In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 3-Q. 2(a). Rings are used in high-performance networks where large bandwidth is necessary e.g. time sensitive features such as video and audio. Every computer is connected to the next computer in the ring and each retransmits what it receives from the previous computer hence the ring is an active network. The messages flow around the ring in one direction.

Advantages of ring topology :

1. Every computer gets an equal access to the token.
2. There are no standing waves produced.

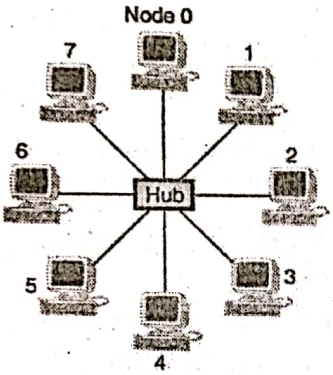
Disadvantages of ring topology :

1. Failure of one computer on the ring can affect the whole network.
2. It is difficult to trouble short the ring.
3. Adding or removing the computers disturbs the network activity.

Scanned by CamScanner

3. Star topology :

- In a star topology all the computers are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 4-Q. 2(a). There is no direct connections among the computers. All the connections are made via the central hub.
- Stars are used in concentrated networks, where the endpoints are directly reachable from a central location; when network expansion is expected and when the greater reliability of a star topology is needed.
- Each computer on a star network communicates with a central hub. The hub then resends the message to all the computers in a broadcast star network. It will resend the message only to the destination computer in a switched star network.



(G-18) **Fig. 4-Q. 2(a) : Star topology**

Advantages of star topology :

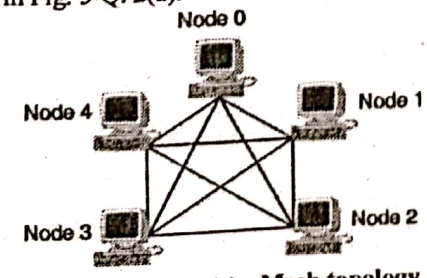
1. It is easy to add new computers to a star network without disturbing the rest of the network.
2. The star network is easy to install and maintain.
3. The fault diagnosis is easy.
4. If a computer or link fails it does not bring down the whole star network.

Disadvantages of star topology :

1. If the central hub fails, the whole network fails to operate.
2. Many star networks require a device at the central point to rebroadcast or switch the network traffic.
3. The cabling cost is more since cables must be pulled from all computers to the central hub.

4. Mesh topology :

- In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 5-Q. 2(a).



(G-21) **Fig. 5-Q. 2(a) : Mesh topology**

- The term dedicated means that the link carries data only between two devices connected on it.
- A fully connected mesh network therefore has n(n–1)/2 physical cables to connect n devices. To accommodate that many links every device on the network must have n–1 input/output ports.
- So too many cables are required to be used for the mesh topology.

Advantages :

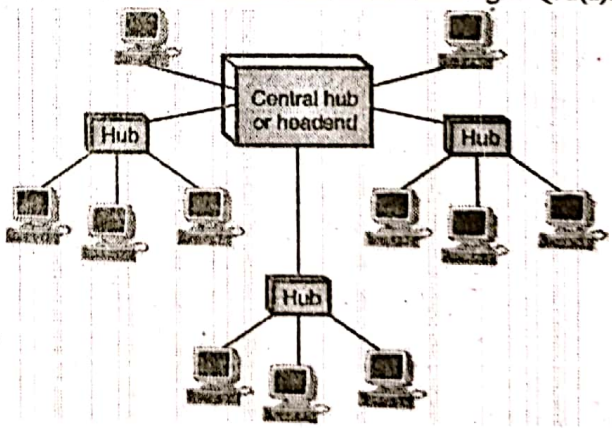
1. The use of dedicated links guarantees that each connection can carry its own data reliably.
2. A mesh topology is robust because the failure of any one computer does not bring down the entire network.
3. It provides security and privacy because every message sent travels along a dedicated line.
4. Point to point links make fault diagnose easy.

Disadvantages :

1. Since every computer must be connected to every other computer installation and reconfiguration is difficult.
2. Cabling cost is more.
3. The hardware required to connect each link input/output and cable is expensive.

5. Tree topology :

- A tree topology is a variation of a star. As in a star, nodes in a tree are connected to a central hub that controls the entire network.
- However, every computer is not plugged into the central hub. Most of them are connected to a secondary hub which in turn is connected to the central hub as shown in Fig. 6-Q. 2(a).



(G-22) **Fig. 6-Q. 2(a) : Tree topology**

- The central hub in the tree is an active hub which contains repeater. The repeater amplify the signal and increase the distance a signal can travel. The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.

Advantages :

1. It allows more devices to be attached to a single hub and can therefore increase the distance of a signal can travel between devices.

Scanned by CamScanner

2. It allows the network to isolate and attach priorities to the communications from different computers.

Disadvantages :

1. If the central hub fails the system breaks down.
2. The cabling cost is more.

Chapter 2 : Physical Layer [Total Marks - 04]

Q. 1(c) List the advantages of fiber optics as a communication medium. (4 Marks)

Ans. :

Advantages of optical fibers :

- Some of the advantages of fiber optic communication over the conventional means of communication are as follows :

1. **Small size and light weight :**

The size (diameter) of the optical fibers is very small (it is comparable to the diameter of human hair). Therefore a large number of optical fibers can fit into a cable of small dismeter.

2. **Easy availability and low cost :**

The material used for the manufacturing of optical fibers is "silica glass". This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.

3. **No electrical or electromagnetic interference :**

Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.

4. **Large bandwidth :**

As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fiber is extremely large. This allows transmission of more number of channels. Therefore the information carrying capacity of an optical fiber is much higher than that of a co-axial cable.

Chapter 3 : Data Link Layer [Total Marks - 14]

Q. 1(e) Explain in short different framing methods. (4 Marks)

Ans. :

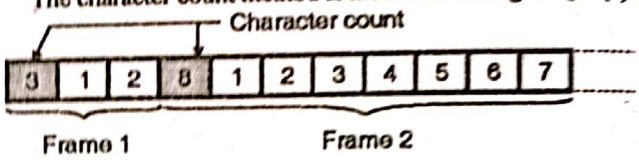
Framing methods :

Following methods are used for carrying out framing :

1. Character count method.
2. Starting and ending characters, with character stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

Character count :

- In this method, a field in the header is used to specify the number of characters in the frame.
- This number helps the receiver to know the exact number of characters present in the frame following this count.
- The character count method is illustrated in Fig. 1-Q. 1(e).

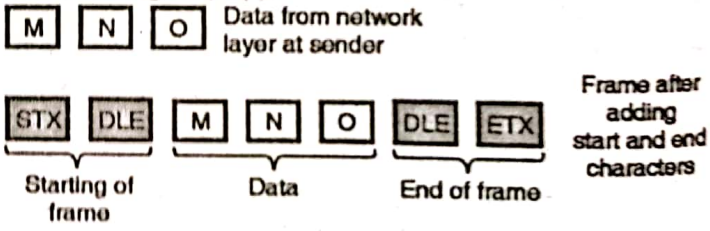


(L-668) **Fig. 1-Q. 1(e) : Character count method**

- The two frames shown in Fig. 1-Q. 1(e) contain 3 and 8 characters respectively and numbers 3 and 8 are inserted in the headers of the corresponding frames. The disadvantage of this method is that, an error can change the character count itself.
- If the wrong character count number is received due to error then the receiver will get out of synchronization and will not be able to locate the start of next frame. The character count method is rarely used in practice.

Starting and ending character with character stuffing :

The problem of character count method is solved here by using a starting character before the starting of each frame and an ending character at the end of each frame. Each frame is preceded by the transmission of ASCII character sequence DLE STX. (DLE stands for data link escape and STX is start of TeXt). After each frame the ASCII character sequence DLE ETX is transmitted. Here DLE stands for Data Link Escape and ETX stands for End of TeXt. So if the receiver loses the synchronization, it just has to search for the DLE STX or DLE ETX characters to return back on track. This is shown in Fig. 2-Q. 1(e).



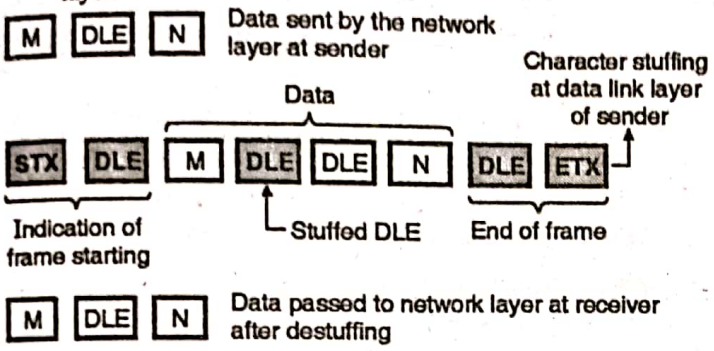
(L-669) **Fig. 2-Q. 1(e)**

Character stuffing :

- The problem with this system is that the characters DLE STX or DLE ETX can be a part of data as well.
- If so, they will be misinterpreted by the receiver as start or end of frame.
- This problem is solved by using a technique called **character stuffing** which is as follows.

Scanned by CamScanner

- The data link layer at the sending end inserts an ASCII DLE character just before each accidental DLE character in the data being transmitted.
- The data link layer at the receiving end will remove these DLE characters before transferring the data to the network layer.



(G-181) **Fig. 3-Q. 1(e) : Character stuffing**

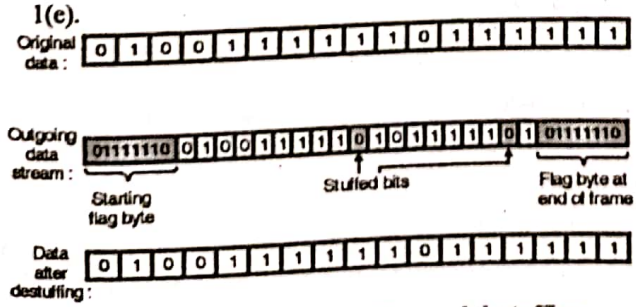
- Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once.
- This is called character stuffing and it is shown in Fig. 3-Q. 1(e). Note that at the receiving end the destuffing is essential. Destuffing process is exactly opposite to the character stuffing process.

Starting and ending flags, with bit stuffing :

- In this framing techniques at the beginning and end of each frame, a specific bit pattern 0111 1110 called **flag byte** is transmitted by the sending station.
- Since there are six consecutive 1s in the flag byte a technique called **bit stuffing** which is similar to character stuffing is used. It is as explained below.

Bit stuffing :

- Whenever the sender data link layer detects the presence of five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing bit stream. Thus the six consecutive 1s will never appear in the data stream. Hence there is no chance of misinterpretation.
- This is called bit stuffing and it is illustrated in Fig. 4-Q. 1(e).



(G-183) **Fig. 4-Q. 1(e) : Bit stuffing and destuffing**

- When a receiver detects presence of five consecutive ones in the received bit stream, it automatically deletes the 0 bit following the five ones. This is called de-stuffing. It is shown in Fig. 4-Q. 1(e).
- Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

Q. 5(a) Explain the use of TCP timers in detail. (10 Marks)

Ans. :

Use of TCP timer :

- As soon as a sender transmits a frame, it also starts the data link timer. The timer timing is set by taking into account the factors such as the time required for the frame to reach the destination, processing time at the destination and the time required for the acknowledgement to return back. Normally the frame is received correctly and the acknowledgement will return back to the sender before the timer runs out.
- This shows that a frame has been received and the timer is cancelled.
- But if a frame is lost or acknowledgement is lost, then the timer will go off. This will alert the sender that there is some problem.
- The solution to this problem is that the sender retransmits the same frame.
- But when a frame is transmitted multiple times, there is a possibility that the receiver will receive the same frame two or more times and pass it to the network layer more than once. This is called as duplication.
- To avoid this each outgoing frame is assigned a distinct sequence number. This will help the receiver to distinguish retransmission.

Chapter 4 : Medium Access Control Layer & LAN [Total Marks - 20]

Q. 3(a) Explain CSMA protocols. Explain how collision are handled in CSMA / CD. (10 Marks)

Ans. :

Carrier Sense Multiple Access (CSMA) :

The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-persistent CSMA :

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.

Scanned by CamScanner

1-Persistent CSMA :

- In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.
- The disadvantage of this strategy is that if two stations are waiting then they will transmit simultaneously and collision will take place. This will then require retransmission.

P-Persistent CSMA :

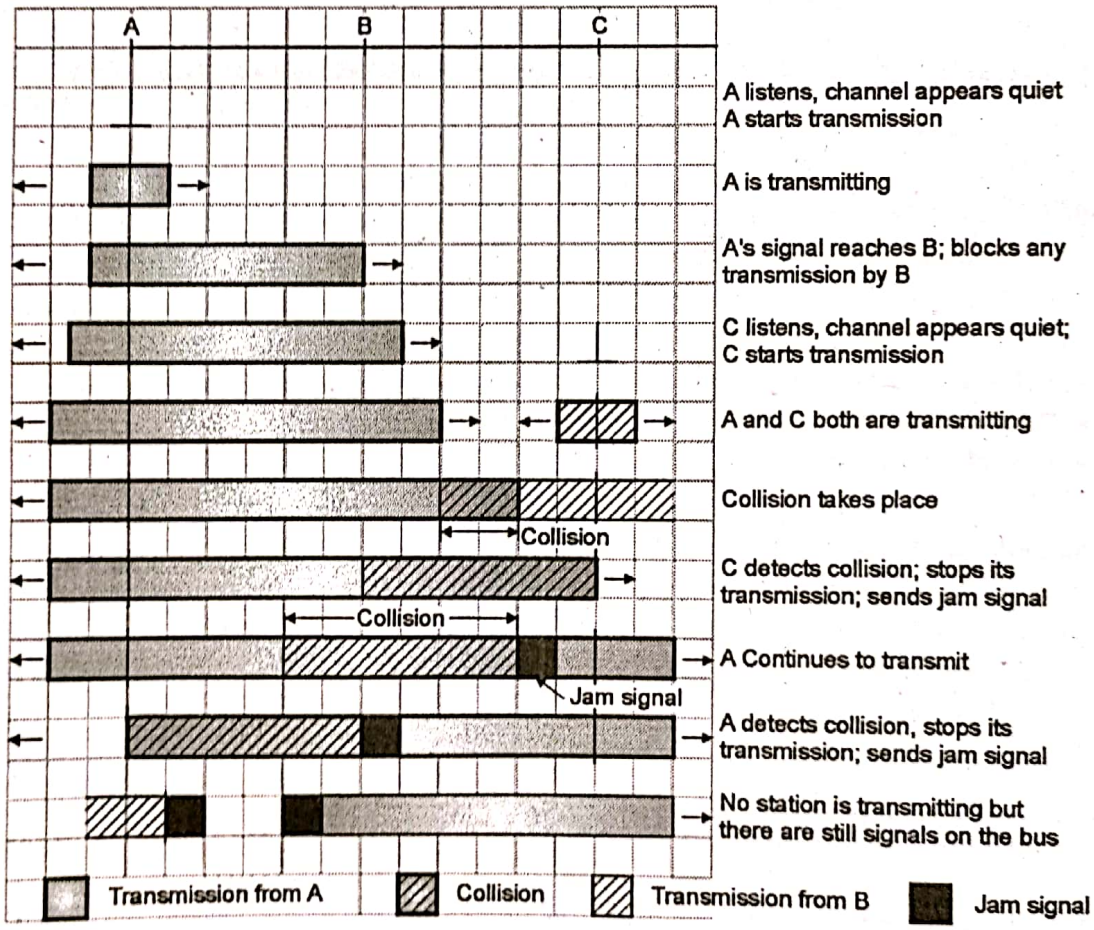
- The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.
- A station is assumed to be transmitting with a probability "p". For example if p = 1/6 and if 6 stations are waiting then on an average only one station will transmit and others will wait.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

- The problem in CSMA is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.
- As soon as a collision is detected, the transmitting stations release a jam signal.
- The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.



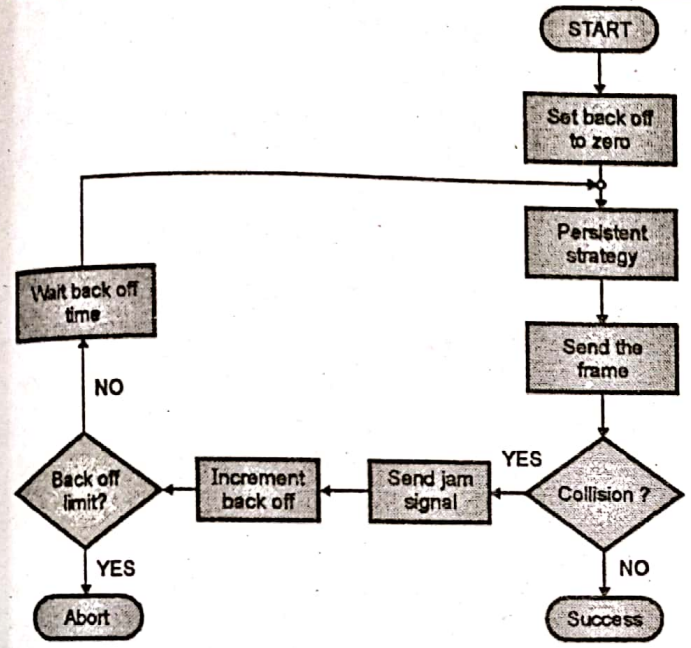
(G-273)**Fig. 1-Q. 3(a) : CSMA/CD scheme**

- Otherwise there is a possibility that the same frames would collide again. After some "back off" delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively. A careful design can achieve efficiencies of more than 90% using CSMA/CD. This scheme is as shown in Fig. 1-Q. 3(a).

CSMA/CD procedure :

- Fig. 2-Q. 3(a) shows a flow chart for the CSMA/CD protocol.

Scanned by CamScanner



(G-276)Fig. 2-Q. 3(a) : CSMA/CD procedure

Explanation :

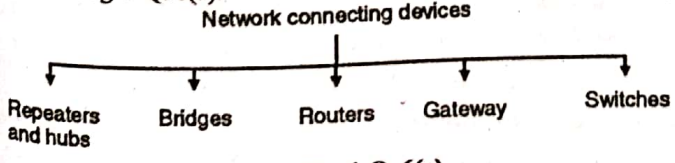
- The station that has a ready frame sets the back off parameter to zero.
- Then it senses the line using one of the persistent strategies.
- It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.
- If the back off has reached its limit then the station aborts the transmission.
- CSMA/CD is used for the traditional Ethernet.
- CSMA/CD is an important protocol. IEEE 802.3 (Ethernet) is an example of CSMA/CD. It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

Q. 6(a) Write a short note on the : Internetworking devices (10 Marks)

Ans. :

Network connecting devices :

- Different types of network connecting devices are as shown in Fig. 1-Q. 6(a).

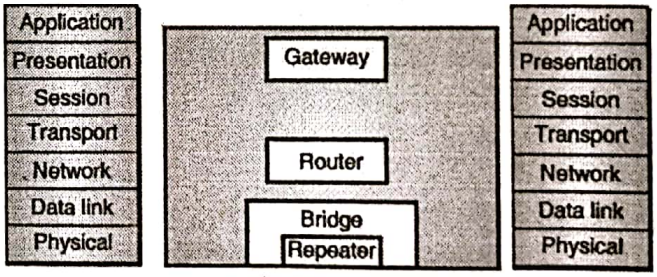


(G-348) Fig. 1-Q. 6(a)

- The relation between OSI reference model and various connecting devices is shown in Fig. 2-Q. 6(a).

Network connecting devices :

- Two or more devices are connected to each other for the purpose of sharing data or resources from a network.
- A LAN may be spread over a larger distance than its media can handle effectively. The number of stations also can be more than a number which can be handled and managed properly. Such networks should be subdivided into smaller networks and these smaller subnetworks should be connected to each other through connecting devices.
- A device called a repeater is inserted into the network to increase the coverable distance or a device called a bridge can be inserted for traffic management.
- When two or more separate networks are connected for exchanging data or resources it creates an internetwork. Routers and gateways are used for internetworking.
- Each of these device type interacts with protocols at different layers of the OSI model.
- Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer.
- Bridges utilize addressing protocols and can affect the flow control of a single LAN. Bridges are most active at the data link layer.
- Routers provide links between two separate but same type LANs and are active at the network layer.
- Finally gateways provide translation services between incompatible LANs or applications and are active in all of the layers. Connecting devices and the OSI model is shown in Fig. 2-Q. 6(a).



(G-806(a)) Fig. 2-Q. 6(a) : Connecting devices and OSI model

- Categories of connecting devices :
- Fig. 2-Q. 6(a) shows the relationship between the connecting devices and various layers of the internet model.

Table 1-Q. 6(a) : Role of networking devices

Sr. No.	Name of the device	Role
1.	Passive hub	Operate below the physical layer.
2.	Repeater	Regenerates the original signal. Operates in the physical layer.

Scanned by CamScanner

Sr. No.	Name of the device	Role
3.	Bridge	Bridges utilize the address protocol. They can carry out the traffic management. They are most active in the data link layer.
4.	Routers	Routers provide connections between two seperate but compatible networks. It works in the network layer.
5.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.

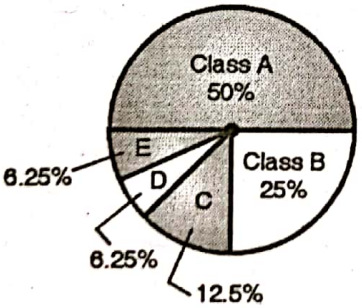
Chapter 5 : Network Layer
[Total Marks - 68]

Q. 1(d) Explain with examples the classification of IPv4 addresses. (4 Marks)

Ans. :

Classification of IPv4 addresses:

- In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E.
- Fig. 1-Q. 1(d) shows the percentage of occupation of the address space by each class.
- The number of class A addresses is the highest i.e. 50% and those of classes D and E is the lowest i.e. 6.25%.



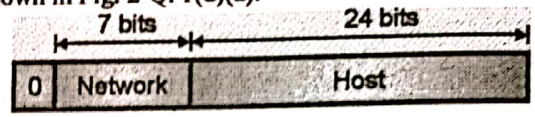
Class	No. of addresses	
A	2^{31}	50%
B	2^{30}	25%
C	2^{29}	12.5%
D	2^{28}	6.25%
E	2^{28}	6.25%

(G-2003) Fig. 1-Q. 1(d) : Classful addressing occupation of address space

Formats of various classes :

Class A format :

- The formats used for IPv4 address are as shown in Fig. 2-Q. 1(d)(a). The IPv4 address for class A networks is shown in Fig. 2-Q. 1(d)(a).

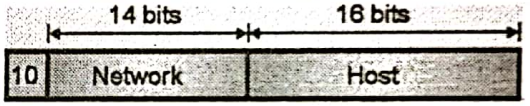


(G-531) Fig. 2-Q. 1(d)(a) : Class A IPv4 address formats

- But the host numbers will range from 0.0.0.0 to 127.255.255.255.
- Thus in class A, there can be 126 types of networks and 17 million hosts.

Class B format :

- The class B address format is shown in Fig. 2-Q. 1(d)(b).
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.



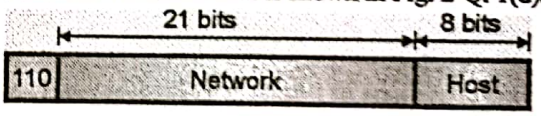
(G-532) Fig. 2-Q. 1(d)(b) : Class B format

- Class B networks are large. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65,534 (216-2) hosts in a class B network. Most of the 16,382 class B addresses have been allocated. The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

Example : 128.89.0.26, for host 0.26 on net 128.89.

Class C format :

- The class C address format is shown in Fig. 2-Q. 1(d)(c).



(G-533) Fig. 2-Q. 1(d)(c) : Class C format

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 2-Q. 1(d)(d).

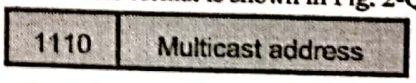


Fig. 2-Q. 1(d)(d) : Class D format

- The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 2-Q. 1(d)(e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

Scanned by CamScanner

11110	Reserved for future use

Fig. 2-Q. 1(d)(e) : IPv4 address for class E network

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

Q. 1(f) Explain the need of subnet mask in subnetting. (4 Marks)

Ans. :

Subnetting :

- The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host.
- But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :

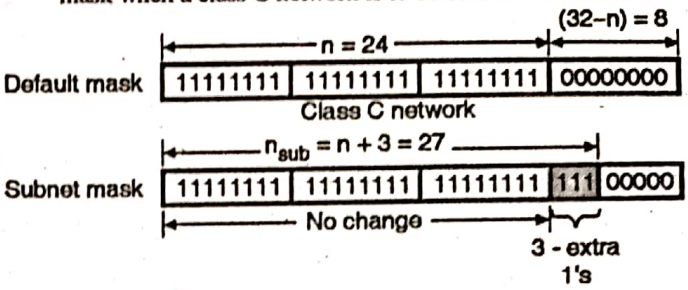
1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

Definition of subnetting :

- We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses.
- In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets.**
- Each such subnet has its own **subnet address.**

Subnet mask :

- The **network mask** or **default** mask are used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting** is **not** to be done.
- But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet.
- Fig. 1-Q. 1(f) shows the format of a subnet mask. Each subnet has its own **net id** and **host id.**
- If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 1-Q. 1(f).
- In Fig. 1-Q. 1(f), we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.



(G-2011) **Fig. 1-Q. 1(f) : Default and subnet masks**

Q. 2(b) What is IPv4 protocol ? Explain the IPv4 header format with diagram. (10 Marks)

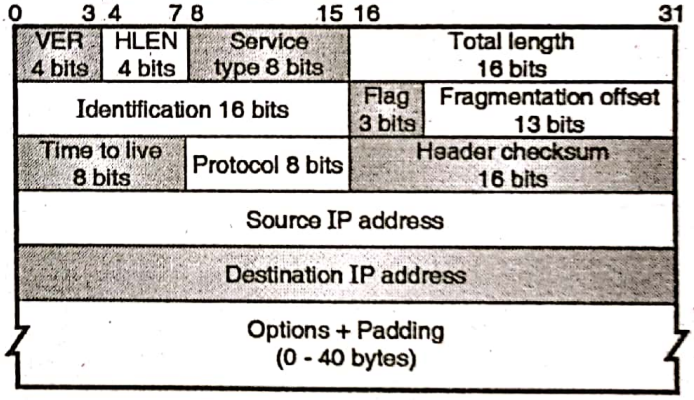
Ans. :

Internet protocol (IP) :

The Internet Protocol is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.

IPv4 header format :

The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure is as shown in Fig. 1-Q. 2(b).



(G-2082) **Fig. 1-Q. 2(b) : IPv4 header format**

Various fields in the header format are as follows :

1. **VER (Version) :**

- This is a 4 bit field which is used to define the version of IP protocol. The current version of IP is 4 i.e. IPv4 but in future it may be completely replaced by the latest version of IP i.e. IPv6.
- This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version.
- If the processing machine is using some other version of IP, then the datagram will be discarded.

2. **HLEN (Header length) :**

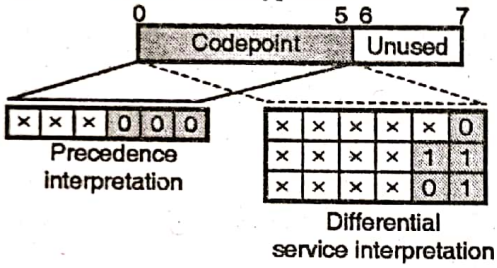
- This 4-bit long field is used for defining the length of the datagram header in 4-byte words.

Scanned by CamScanner

- The value of this field is multiplied by 4 to get the length of the IPv4 header which varies between 20 and 60 bytes.
- When there are no options, the value of this field is 5 and the **header length** is $5 \times 4 = 20$ bytes.
- When the value of option field is maximum the value of HLEN field is 15 and the corresponding header length is maximum i.e. $15 \times 4 = 60$ bytes.

3. Service type :

- In the IP header, this field was called as **Type of Service (TOS)** field and its job was to define how the datagram should be handled.
- At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc.
- But now the interpretation of this field has been changed by IETF. This field is now supposed to define a set of differential services. Fig. 2-Q. 2(b) illustrates the new interpretation of the **service type** field.



(G-2083) **Fig. 2-Q. 2(b) : New interpretation of service type field**

- As seen in Fig. 5.13.4, in the new interpretation, the service type field is divided into two subfields namely, the 6 bit **codepoint** subfield and a 2 bit **unused** subfield.
- We can use the 6-bit **codepoint** subfield in two different ways, as follows :

1. For the purpose of precedence interpretation.
2. For the differential service interpretation.

Precedence interpretation :

- If the three right most bits are zeros, then the three leftmost bits are interpreted the same as the precedence bits in the service field (old interpretation). That means it is compatible with the old interpretation of this field.
- The precedence interpretation is used for defining the priority level of this datagram (from 0 to 7) in the situations like congestion.
- In the event of congestion, the datagrams with lowest precedence (0) will be discarded first.

Differential service interpretation :

- When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation.
- In that case these 6 bits can be used for defining a total of 56 (64 – 8) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 5.13.1.

Table 1-Q. 2(b) : Values of codepoints

Category	Codepoint	Assigning authority
1.	× × × × × 0	Internet
2.	× × × × 1 1	Local
3.	× × × × 0 1	Temporary or Experimental

- The first, second and third categories contain 24, 16 and 16 service types respectively.
- The Internet authorities assign the first category. The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

- This 16 bit field is used to define the total length of the IP datagram. The total length includes the length of header as well as the data field.
- The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1) = 65535$ bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers.
- This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.
- All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments.
- The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram.
- We can find the length of data by subtracting the header length from the total length.
- The header length can be obtained by multiplying the contents of HLEN field by four.

$\therefore$ Length of data = Total length – header length

- The total length (maximum value) of 65,535 bytes might seem to be large but in future the size of IP datagram is likely to increase further because the improvement in technology will allow more bandwidth.

Why do we need the total length field ?

- We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame. Then why to include this field ?
- The answer to this question is that in many situations we do not need this field at all.

Scanned by CamScanner

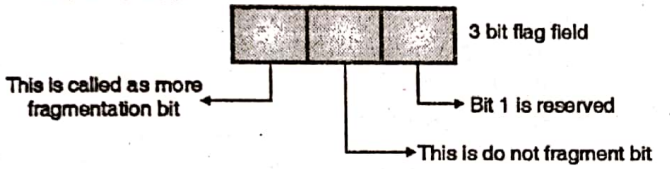
- But in some special situations, only the datagram is not encapsulated in the frame but there are some padding bits as well that are included.
- In such situations, the machine (host or router) that decapsulates the datagram, needs to check the **total length** field so as to understand how much is the data and how much is the padding ?

5. Identification :

- This field is used to identify the datagram originating from the source host. When a datagram is fragmented, the contents of the identification field get copied into all fragments. This identification number is used by the destination to reassemble the fragments of the datagram.

6. Flags :

- **Flags :** This is a three bit field. The 3 bits are as shown in Fig. 3-Q. 2(b).

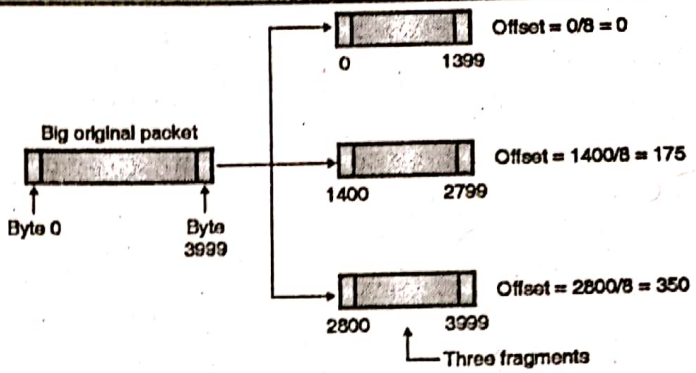


(G-527)**Fig. 3-Q. 2(b) : Flag bits**

- First bit is reserved, and it should be 0.
- The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented.
- But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.
- The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. Fragmentation offset :

- This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- To understand this refer Fig. 4-Q. 2(b).
- The original IP packet (datagram) contains 4000 bytes numbered from 0 to 3999. It is fragmented into three fragments.
- The first fragment contains 1400 bytes numbered from 0 to 1399. The offset for this fragment is 0/8 = 0. Similarly the offsets for the other two fragments are 1400/8 = 175 and 2800/8 = 350 respectively as shown in Fig. 4-Q. 2(b).
- The offset is measured in units of 8 bytes. Because the length of the offset field is 13 bits, so the fragments should be of size such that first byte number is divisible by 8.



(G-528) **Fig. 4-Q. 2(b) : Example of fragmentation**

8. Time to live (TTL) :

- This is an 8-bit field which controls the maximum number of routers visited by the datagram during its lifetime.
- A datagram has a limited lifetime for travelling through an Internet.
- Originally the TTL field was designed to hold the **timestamp.** This timestamp value was decremented by one, everytime the datagram visits a router.
- As soon as the timestamp value reduces to zero the datagram is discarded. But for this scheme to become successful, all the machines must have synchronized clocks and they must know the time taken by a datagram to travel from one router to the other.
- Today the TTL field is used to **control** the maximum number of hops i.e. router by a datagram.
- At the time of sending a datagram, the source host will store a number in the TTL field. This number is approximately twice the maximum number of routers present between any two hosts.
- Everytime this datagram visits a router, this value is decremented by one. If after decrementing, the value of TTL field reduces to zero then that router discards the datagram.

9. Protocol :

- This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer.
- The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.
- The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered.
- At the destination, the value of this field helps in the process of demultiplexing.
- Table 2-Q. 2(b) shows some of the values of this field corresponding to different high level protocols.

Scanned by CamScanner

Table 2-Q. 2(b)

Value	Protocol	Value	Protocol
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

10. Header checksum :

A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

11. Source address :

This field is used for defining the IP address of the source. It is a 32 bit field.

12. Destination address :

This field is used for defining the IP address of the destination. It is also a 32 bit field.

13. Options :

Options are not required for every datagram. They are used for network testing and debugging.

Q. 3(b) What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. (10 Marks)

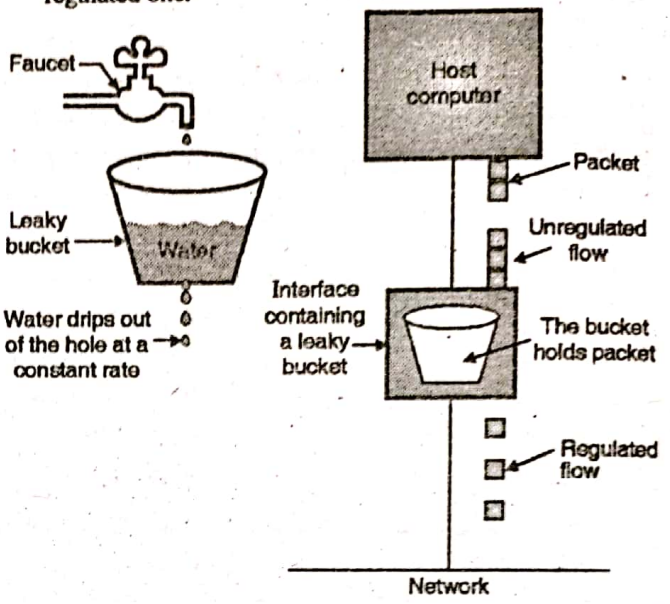
Ans. :

Traffic shaping :

- Traffic shaping is an open loop control of congestion control. It manages the congestion by making the packet transmission rate to be more predictable. This will make the data rate more uniform and bursty traffic is reduced.Thus traffic shaping will regulate the average rate or the burstiness of data transmission.The process of monitoring a traffic flow is called as **traffic policing.**

Leaky bucket algorithm :

- Leaky bucket algorithm is used to control congestion in network traffic. As the name suggests it's working is similar to a leaky bucket in real life.
- The principle of leaky bucket algorithm is as follows :
- Leaky bucket is a bucket with a hole at bottom. Flow of the water from bucket is at a constant rate (data rate is constant) which is independent of water entering the bucket (incoming data). If bucket is full, any additional water entering in the bucket is thrown out (Packets are discarded).
- Same technique is applied to control congestion in network traffic. Every host in the network is having a buffer (equivalent to a bucket) with finite queue length.
- Packets which are put in the buffer when buffer is full are thrown away. The buffer may send some number of packets per unit time onto the subnet (helpful if packets vary greatly in size) as shown in Fig. 1-Q. 3(b) the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.

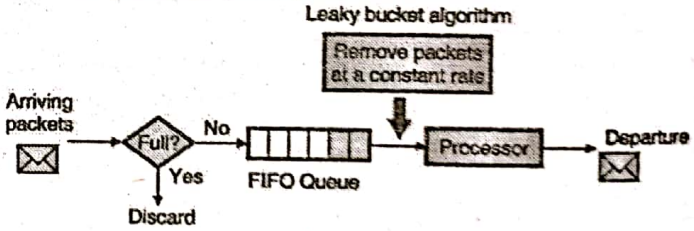


(G-481) **Fig. 1-Q. 3(b) : Leaky bucket algorithm**

Leaky bucket implementation :

- Fig. 2-Q. 3(b) shows the implementation of leaky bucket principle. A FIFO (First In First Out) queue is used for holding the packets which is equivalent to the leaky bucket.
- Two different operating conditions for the implementation of Leaky bucket are as follows:

1. For packets of fixed size.
2. For packets of variable size.



(G-482) **Fig. 2-Q. 3(b) : Implementation of leaky bucket**

1. Fixed size packets :

If the arriving packets are of fixed size (e.g. cells in ATM networks), then the process of Fig. 2-Q. 3(b) will allow the removal of a fixed number of packets from the queue corresponding to every tick of the clock.

2. Packets of variable size :

If the packets at the input of the process are of different size, then the fixed output rate will not correspond to the number of packets leaving the process but it will correspond to the number of bits leaving the process.

Algorithm :

The algorithm for variable length packets is as follows :

1. Initialize a counter to a number "n" at the tick of the clock.
2. If "n" is greater than the packet size, then send the packet and decrement the counter by the packet size.

Scanned by CamScanner

3. Repeat step 2 until "n" becomes smaller than the packet size.
4. Reset the counter and go back to step 1.

Comparison of token bucket and leaky bucket :

Table : 1-Q. 3(b) : Comparison of token bucket and leaky bucket

Sr. No.	Leaky bucket	Token bucket
1.	Smooth out traffic by passing packets only when there is a token. Does not permit burstiness.	Token bucket smooths traffic too but permits bustiness.
2.	Leaky bucket discards packets for which no tokens are available. (No concept of queue)	Token bucket discards token when bucket is full, but never discards packets (infinite queue)
3.	Application : Traffic shaping or traffic policing.	Application : Network traffic shaping or rate limiting

Q. 4(a) What is ICMP protocol ? Explain the ICMP header format with diagram. (10 Marks)

Ans. :

ICMPv4 (Internet Control Message Protocol) :

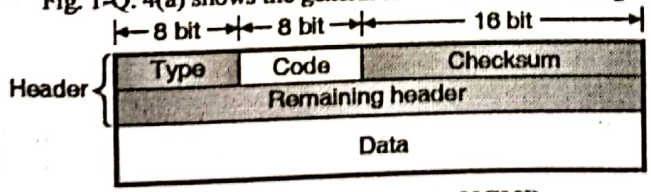
- The IP provides unreliable and connectionless datagram delivery, and makes an efficient use of network resources.
- IP is a best-effort delivery (which does not provide any guarantee) service that takes a datagram from its original source to its final destination. However, IP has two drawbacks :

1. It does not have any error control mechanism.
2. It does not have any assistance mechanism.

- The Internet Control Message Protocol (ICMP) is used to overcome these drawbacks. It is used alongwith IP. It reports presence of errors and sends the control messages on behalf of IP.

ICMP header format :

- Fig. 1-Q. 4(a) shows the general format of ICMP messages.



(G-2105) **Fig. 1-Q. 4(a) : General format of ICMP messages**

- As shown in Fig. 1-Q. 4(a), the header of an ICMP message is 8-byte long and the data section is of a variable size.
- The general header format for each ICMP message is different. But the first four bytes are common to all the message types.

1. **Type :**
   This 8-bit field is used for defining the types of message.
2. **Code :**
   This 8-bit field is used for specifying the reason for the particular message type.

- The last common field is the **checksum** field which is 16 bit (2 byte) long. The information to find the original packet that had error is included in the **data section** of the error messages.
- Whereas the **data section** in the query messages contains extra information depending on the type of query.

Q. 5(b) Compare open loop congestion control and closed loop congestion control. (10 Marks)

Ans. :

Principle of congestion control :

- The solutions to the congestion problems can be divided into two categories or groups as open loop solutions and closed loop solutions.
- Congestion control refers to the techniques and mechanisms which can either prevent congestion from happening or remove congestion after it has taken place.
- The **open loop congestion** control is based on the prevention of congestion whereas the **closed loop solutions** are for removing the congestion after it has occurred.

Open loop control :

- Open loop solutions try to solve the congestion issue by excellent design to prevent the congestion from happening.
- Open loop control is exercised by using the tools such as deciding when to accept the new packets, when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points.
- It is important to note that none of these decisions are made on the basis of the current status of a network, as no feedback is being used.

Closed loop control :

- The closed loop congestion control uses some kind of feedback. It takes into account the current status of the network.
- A closed loop control is based on the following three steps :

1. Detect the congestion and locate it by monitoring the system.
2. Transfer the information about congestion to places where action can be taken.
3. Adjust the system operations to correct the congestion.

Two examples of closed loop control are :

1. TCP flow control.
2. BR rate control for an ATM network.

Scanned by CamScanner

Open loop versus closed loop :

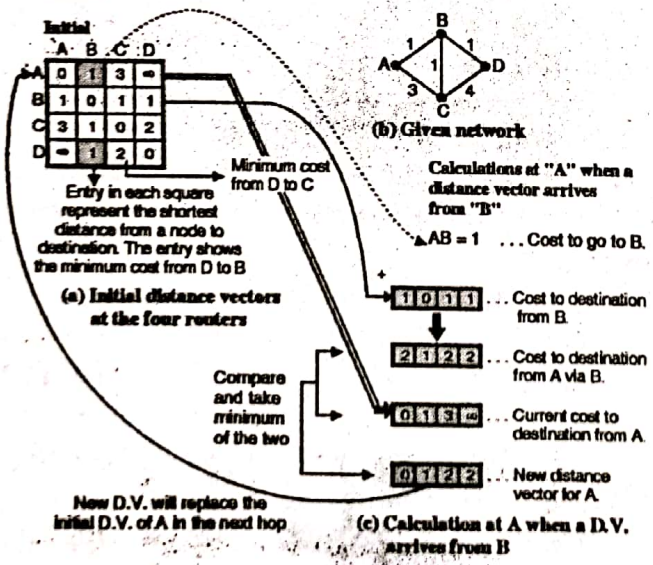
- Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control.
- In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.
- Some people feel that closed loop congestion control schemes are too slow in today's high-speed, large range network. Because it takes a long time for feedback to go back to source. Hence before any corrective action takes place thousands of packets have been already lost.
- But on other hand, if the congestion has already taken place and the overload is of long duration, the congestion cannot be released unless the source causing the congestion is asked to reduce its rate.
- Furthermore, ABR service is designed to use any bandwidth that is left over the source must have some knowledge of what is available when it is sending cells.

Q. 6 (b) Write a short note on distance vector routing. **(10 Marks)**

Ans. :

Distance vector routing algorithm :

- In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there.



(G-462) **Fig. 1-Q. 6(b) : Distance vector algorithm at router A**

This algorithm is sometimes called by other names such as :

1. Distributed Bellman-Ford routing algorithm.
2. Ford-Fulkerson algorithm

- In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet.

This entry has two parts :

1. The first part shows the preferred outgoing line to be used to reach the specific destination.
2. Second part gives an estimate of the time or distance to that destination.

Distance vector :

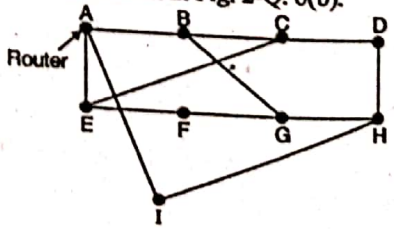
- In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known.
- A **distance vector** is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance vector.
- The cost in each tuple is equal the sum of costs on the shortest path to the destination.

Updation of router tables :

- A router periodically sends a copy of its distance vector to all its neighbours.
- When a router receives a distance vector from its neighbour, it tries to find out whether its cost to reach any destination would decrease if it routed packets to that destination through that particular neighbouring router. This is illustrated in Fig. 1-Q. 6(b).
- Fig. 1-Q. 6(b) shows how the D.V. at A is automatically modified when a D.V. is received from B.
- A similar calculation takes place at the other routers as well. So the entries at every router can change. In Fig. 1-Q. 6(b)(a) the initial distance vector is shown. The entries indicate to the costs corresponding to the shortest distance between the routers indicate to that square.
- For example, AC = 3 indicates the cost corresponding to the shortest path in terms of number of hops from A to C.
- Even if nodes asynchronously update their distance vectors the routing tables eventually converge.
- The well known example of distance vector routing is the Bellman-Ford algorithm.

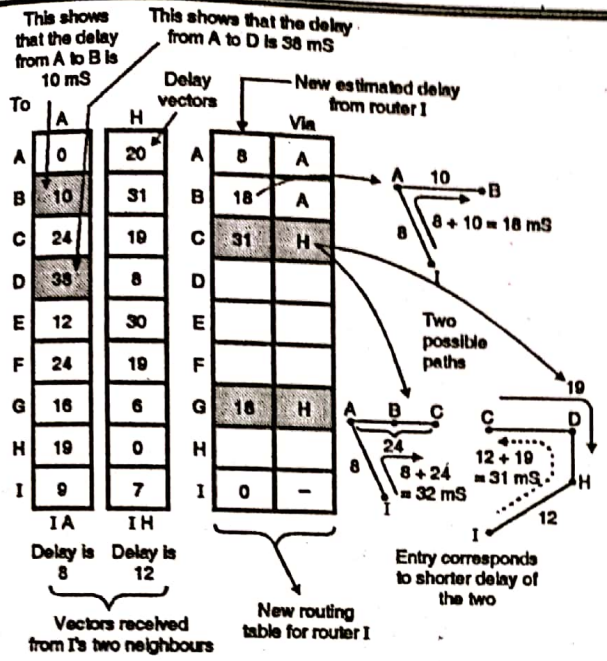
Routing procedure in distance vector routing :

- The example of a subnet is shown in Fig. 2-Q. 6(b) and the routing tables are shown in Fig. 2-Q. 6(b).



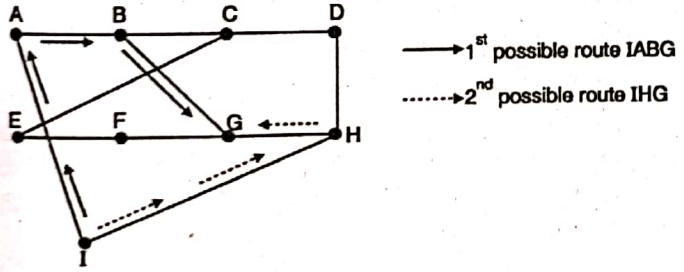
(G-464) **Fig. 2-Q. 6(b) : A subnet**

Scanned by CamScanner



(G-465) Fig. 2-Q. 6(b) : Routing tables

- The entries in router tables of Fig. 2-Q. 6(b) are the delay vectors. For example consider the shaded boxes of Fig. 2-Q. 6(b).
- The entry in the first shaded box shows that the delay from A to B is 10 msec, whereas the entry in the other shaded box indicates that the delay from A to D is 38 msec.
- Consider how router I computes its new route to router G. Fig. 2-Q. 6(b) shows the two possible routes between I and G.



(G-466) Fig. 2-Q. 6(b)

I knows that the reach G via A, the delay required is :

I to A Delay = 8mS
A to G Delay = 16mS
} ∴ I to G Delay = 8 + 16 = 24 msec

(L-891)

Whereas the delay between I and G via H (route IHG) is :

I to H Delay = 12mS
H to G Delay = 6mS
} ∴ I to G Delay = 12 + 6 = 18 msec

(L-892)

- The best of these values is 18 msec corresponding to the path IHG. Hence it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H.
- The new routing table for router I is shown in Fig. 2-Q. 6(b).
- Similarly we can calculate the delays, from I to different destinations from A to I and enter the minimum possible delay into the I's router table.

Q. 6 (c) Write a short note on ARP/RARP. (10 Marks)

Ans. :

Address Resolution Protocol (ARP) :

- The IP protocol is supposed to deliver a packet from the source host to destination host via different routers over the Internet.
- The first step in this entire process is that the IP protocol should know how to deliver the packet to the next hop (router).
- In order to do this, the IP packet should refer to its routing table to find the IP address of the next hop.
- However, IP is using the services of the data link layer. Therefore IP must know the physical address of the next hop (knowing only its IP address won't be enough).
- Thus the IP address of the next hop must be converted (or mapped) into its physical address. This mapping can be done using the protocol called address resolution protocol or ARP.

The Reverse Address Resolution Protocol (RARP) :

- ARP is used for solving the problem of finding out which Ethernet address corresponds to a given IP address. That means ARP is used for the mapping of IP address to physical or MAC address.
- But sometimes we have to solve a reverse problem. That means we have to obtain the IP address corresponding to the given Ethernet (MAC) address.
- Such a problem can occur when booting a diskless workstation.
- The problem of obtaining the IP address when an Ethernet address is given, can be solved by using RARP (Reverse Address Resolution Protocol).
- The newly booted workstation is allowed to broadcast its Ethernet address. The RARP server after receiving this request, checks the Ethernet address in its files and finds the corresponding IP address. This IP address is then sent back.
- The disadvantage of RARP is that it uses a destination address of all 1s (limited broadcasting) to reach the RARP server.
- But such broadcasts are not forwarded by routers, so a RARP server is needed on each network.
- In order to get around this problem, another bootstrap protocol called BOOTP has been invented.
- Unlike RARP, it uses UDP messages which are forwarded over routers. It also provides a diskless workstation with additional information, including the IP address of the file server holding the memory image, the IP address of the default router and the subnet mask to use.

Scanned by CamScanner

Chapter 6 : Transport Layer [Total Marks - 10]

Q. 1(b) Write a program for client server application Using Socked Programming (UDP). (10 Marks)

Ans. :

Socket Programming with UDP :

- When two processes communicate over a TCP connection, it is equivalent to communicating over a virtual pipe between the two processes.
- This pipe will remain in place until one of the processes terminates the TCP connection.
- The sending process does not have to insert the destination address to the bytes to be sent because the virtual connection is existing.
- Also the pipe provides a reliable byte transfer without altering the sequence in which the bytes are received.
- Like TCP, the UDP also allows two or more processes running on different hosts to communicate. But there is a major difference.
- The first difference is that UDP provides a connectionless service so there is no handshaking process in order to establish the virtual pipe like TCP.
- As there is no virtual pipe existing, when a process wants to send a batch of bytes to the other process, the sending process has to attach the address of the destination process.
- The destination address is a tuple consisting of the IP address of the destination host and the port number of the destination process. The IP address and port number together are called as **"packet".**
- UDP provides an unreliable message oriented service in which there is no guarantee that the bytes sent by the sending process will reach the destination process.
- After creating a "packet", the sending process will push the packet into the network through a socket. This packet is then driven in the direction of destination process.
- The code for UDP socket programming is different than that for TCP in the following ways :

1. No need for a welcoming socket as no handshaking is needed.
2. No streams are attached to the socket.
3. The sending host has to create packets.
4. The receiving process has to obtain information from each received packet.

Chapter 7 : Application Layer [Total Marks - 10]

Q. 6 (d) Write a short note on SMTP. (10 Marks)

Ans. :

SMTP (Simple Mail Transfer Protocol) :

- In Internet the source machine establishes a connection to port 25 of the destination machine so as to deliver an e-mail.
- An e-mail daemon which speaks SMTP is listening to this port.
- This daemon is supposed to perform the following tasks :

1. Accept the incoming connections, and copy messages from them into appropriate mailboxes.
2. Return an error message to the sender, if a message is not delivered.

- SMTP is a simple ASCII protocol.
- Once a TCP connection between a sender and port 25 of the receiver is established, the sending machine operates as a client and the receiving machine acts as a server.
- The client then waits for the server to take initiative in communication.
- The server sends a line of text which decares its identity and announces its willingness/ unwillingness to receive mail. If the server is not prepared, the client will release the connection, wait for sometime and try again later.
- But if the server is willing to accept e-mail, then the client announces the sender of e-mail and its recipient.
- If such a recipient exists at the destination, then the server tells the client to send the message. The client, then sends the message and the server sends back its acknowledgement.
- No checksums are generally required because TCP provides a reliable byte stream. If there are any more e-mail, then they can be sent now.
- After exchanging all the e-mail, the connection is released.
- SMTP uses numerical codes. The lines sent by the client are marked C : ; and those sent by the server are marked S : ;
- Some of the commands, useful for communication are : HELO, RCTP, DATA, QUIT etc.
- RCTP represents recipient. If only one command is used then the message is being sent to only one recipient. If the command is used many times, then it indicates that the message is sent to more than one recipients.
- In such a case each message is individually acknowledged or rejected.
- The syntax of four character commands for the clients are rigidly specified but the syntax for the replies are not that rigid.
- The SMTP protocol is well defined by RFC 821 but some problems are still present.

Problems in SMTP :

Some of the problems in SMTP are as follows :

1. Some older versions of SMTP are not capable of handling messages longer than 64 kB.
2. If client and server have different time-outs, then one of them may give up when the other is still busy. This will terminate the connection unnecessarily.
3. In rate situations, infinite mailstorms can be triggered.

□□□

Scanned by CamScanner

May 2019

Chapter 1 : Introduction to Networking [Total Marks - 15]

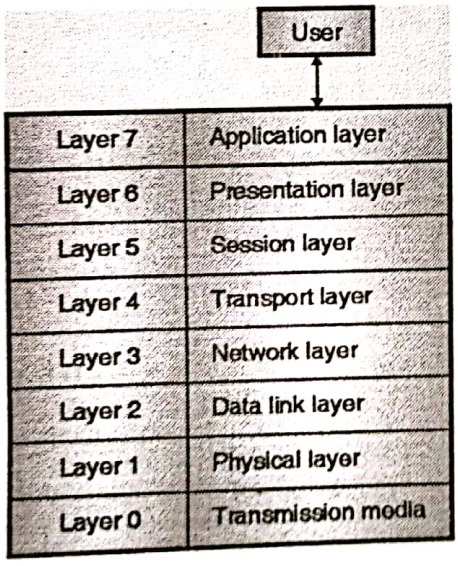
Q. 1 (a) Explain design issues of layers. Explain ISO OSI reference model with diagram. (10 Marks)

Ans. :

Design issues for the OSI layers : Please refer Q. 1(a) of Dec. 2018.

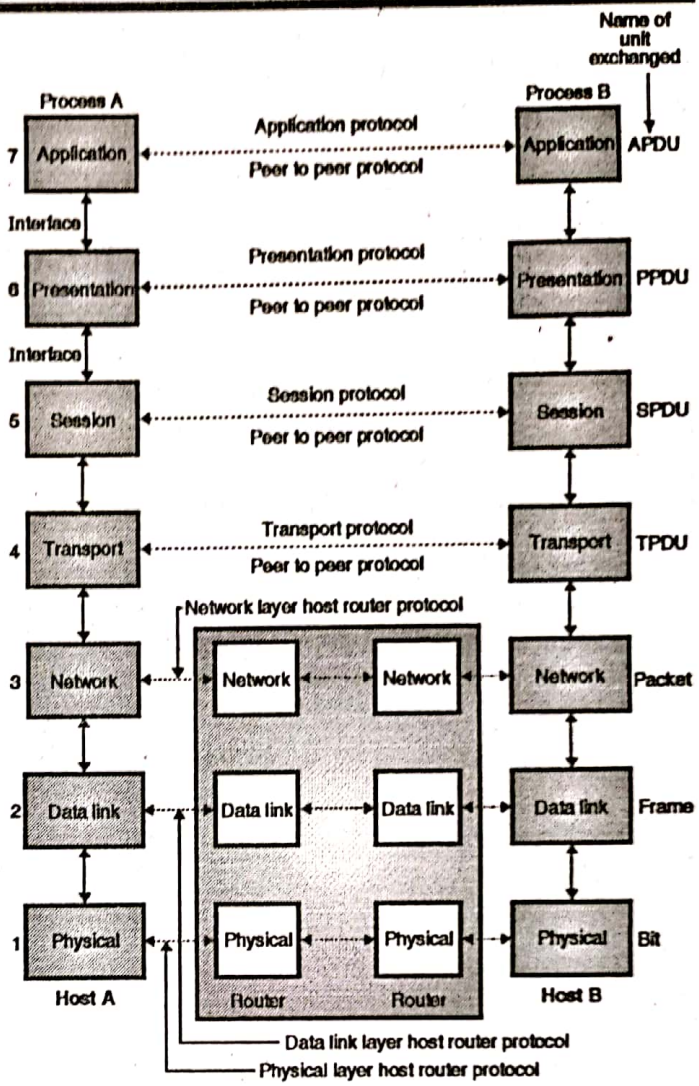
ISO OSI reference model :

- Fig. 1-Q. 1(a) shows the seven layer architecture of ISO-OSI reference model. It defines seven levels or layers in a complete communication system. The lowest layer is physical layer and highest one is called as the application layer.
- A more detailed OSI reference model is shown in Fig. 2-Q. 1(a) The OSI model shown in Fig. 2-Q. 1(a) does not contain the physical medium.



(G-59) **Fig. 1-Q. 1(a): A seven layer ISO-OSI reference model**

- This model is based on a proposal developed by the International Standards Organization (ISO).
- It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e. the systems which are open for communication with other systems.



(G-60) **Fig. 2-Q. 1(a): The OSI reference model**

Table 1-Q. 1(a) shows various layers and its functions.

Table 1-Q. 1(a) : Functions of the layers of ISO-OSI model

Level	Name of the layer	Functions
1.	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2.	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.

Scanned by CamScanner

Level	Name of the layer	Functions
4.	Transport layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session management.
6.	Presentation layer	It works as a translating layer.
7.	Application layer	Retransferring files of information, LOGIN, password checking etc.

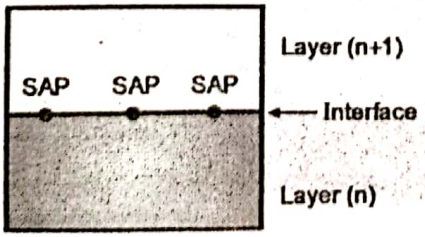
- All the applications need not use all the seven layers shown in Fig. 2-Q. 1(a).
- The lower three layers are enough for most of the applications. Each layer is built from electronic circuits and/or software and has a separate existence from the remaining layers.
- Each layer is supposed to handle message or data from the layers which are immediately above or below it.
- This is done by following the protocol rules. Thus each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

Q. 2 (a) Explain with diagram the relationship between protocol, interface and service. (5 Marks)

Ans. :

Relationship between protocol, interface and service :

- Refer Fig. 1-Q. 2(a) It shows any two layers in the layered structure of a reference model.
- The basic function of each layer is to provide service to the layer above it.



(G-2631) Fig. 1-Q. 2(a)

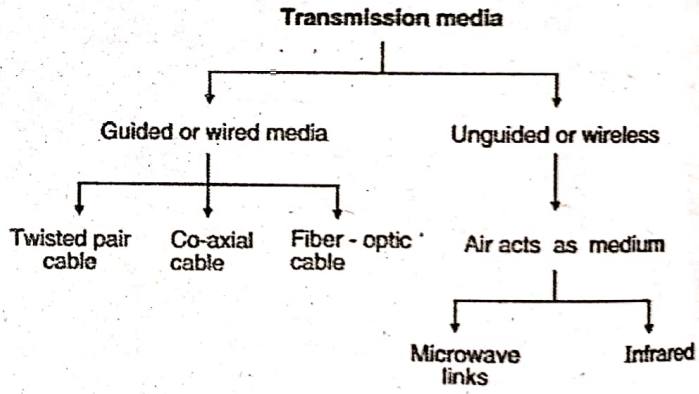
- A service is defined as a set of operations that a layer (n) can provide to the layer above it (n + 1).
- These services are available at SAPs (Service Access Points) at the **interface** of n^{th} and (n + 1) layer as shown in Fig. 1-Q.2(a).
- The SAPs of layer "n" are the places at the interface where the (n + 1) layer can access the services that are being offered by layer "n".
- A **protocol** provides the set of rules for implementing the operations related to the services offered by layer "n" to layer (n + 1).
- This is the relationship between service, interface and protocol.

Chapter 2 : Physical Layer [Total Marks - 10]

Q. 4 (a) Classify transmission media and compare them. (10 Marks)

Ans. :

Classification of transmission media :



(L-571) Fig. 1-Q. 4(a) : Classification of transmission media

Comparison of wired and wireless media :

Table 1-Q. 4(a) : Comparison of wired and wireless media

Sr. No.	Wired media	Wireless media
1.	The signal energy is contained and guided within a solid medium.	The signal energy propagates in the form of unguided electromagnetic waves.
2.	Twisted pair wires, coaxial cable, optical fiber cables are the examples of wired media	Radio and infrared light are the examples of wireless media.

Scanned by CamScanner

Sr. No.	Wired media	Wireless media
3.	Used for point to point communication.	Used for radio broadcasting in all directions.
4.	Wired media lead to discrete network topologies.	Wireless media leads to continuous network topologies.
5.	Additional transmission capacity can be procured by adding more wires.	It is not possible procure additional capacity.
6.	Installation is costly, time consuming and complicated.	Installation needs less time and money.
7.	Attenuation depends exponentially on the distance.	Attenuation is proportional to square of the distance.

Chapter 3 : Data Link Layer
[Total Marks - 25]

Q. 1 (b) Explain design issues of Data link layer. Explain sliding window protocol selective repeat. (10 Marks)

Ans. :

Data link layer design issues (Functions of data link layer) :

1. Services provided to the network layer :

The data link layer provides a well defined service interface to the network layer. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via the DLL.

2. Frame synchronisation :

The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. Flow control :

The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. Error control :

The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. Addressing :

When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames. This is known as addressing.

6. Control and data on same link :

The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to separate out the control information from the data being transmitted.

7. Link management :

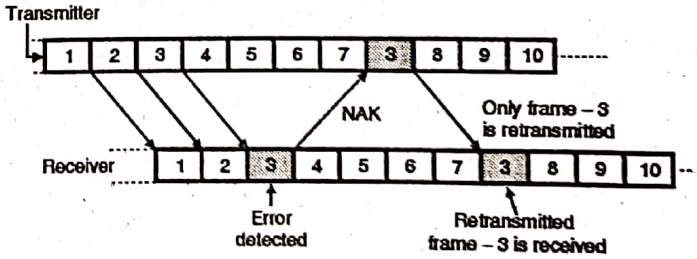
The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data. It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

Selective repeat ARQ :

In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways :

1. The receiver can do sorting of data frames and is also able to store frames received after it has sent the NAK until the damaged frame has been replaced.
2. The transmitter has a searching mechanism that allows it to choose only those frames which are requested for retransmission.
3. The window size in this method is less than or equal to $(n + 1)/2$, whereas in case of go-back-n it is $n - 1$.

The principle of operation of this protocol is illustrated in Fig. 1-Q. 1(b).



(G-243) **Fig. 1-Q. 1(b) : Selective repeat ARQ system**

- In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next frame. It transmits the frames continuously till it receives the "NAK" signal from the receiver.
- The receiver sends the "NAK" signal back to the transmitter as soon as it detects an error in the received frame. For example the receiver detects an error in the third frame, as shown in Fig. 1-Q. 1(b).
- By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 1-Q. 1(b).

Scanned by CamScanner

- On reception of "NAK" signal, the transmitter will retransmit only the frame-3 and then continues with the sequence 8, 9... as shown in Fig. 1-Q. 1(b).
- The frames 4, 5, 6 and 7 received by the receiver which do not contain any error are not discarded by the receiver. The receiver receives the retransmitted frames in between the regular frames. Therefore the receiver will have to maintain the frames sequentially.
- Hence the selective repeat ARQ is the most efficient but the most complex protocol, of all the ARQ protocols.
- Thus in selective repeat ARQ only the frame which is damaged or lost is retransmitted by the transmitter.
- The lost ACK or NAK frames are treated in the same manner as the go-back-n method.
- When the transmitter reaches either the capacity of its window [(n + 1)/2] or the end of its transmission it sets a timer.
- If no acknowledgement arrives in the allotted time, all the frames that remain unacknowledged are retransmitted.

Q. 3 (a) Explain different framing methods. What are the advantages of variable length frame over fixed layer frame ? (10 Marks)

Ans. :

Different framing methods : Please Refer Q. 1(e) of Dec. 2018.

Advantages of variable length frame over fixed layer frame :

1. Although the whole message could be packed in one big frame, it is not done practically because for large frames the flow and error control becomes inefficient. Also even for a single error the whole message needs to be retransmitted. When the same message is divided into smaller frames, the flow and error control become efficient.
2. In LANs there are more than one senders. The messages sent by them could be of different size. Hence it makes system efficient by keeping frame size variable as it is possible to select an optimum frame size as per requirements.

Q. 6 (a) Short note on HDLC. (5 Marks)

Ans. :

High level data link control (HDLC) protocol :

- The high level data link control (HDLC) protocol was developed by ISO.
- It is the most widely accepted data link layer protocol. It has the advantages of flexibility, adaptability, reliability and efficiency of operation.
- HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
- For the HDLC protocol the following three types of stations have been defined :
  1. Primary station 2. Secondary station
  3. Combined station

1. Primary station :

A primary station takes care of the data link management. When communication between the primary and secondary stations takes place, the primary station would connect and disconnect the data link. The frames sent by a primary station are called commands.

2. Secondary station :

A secondary station operates under the control of a primary station. When communication between primary and secondary stations takes place, the frames sent by the secondary station takes place are called responses.

3. Combined station :

A combined station can act as primary as well as secondary stations. Therefore it can send both commands and responses.

Operating modes for data transfer :

- In HDLC both synchronous and asynchronous modes of communication are permitted.
- The meaning of the words synchronous and asynchronous is different from that of a physical layer.
- Following modes of operation are possible for data transfer :
  1. Normal response mode (NRM)
  2. Asynchronous response mode (ARM)
  3. Asynchronous balanced mode (ABM)
- The first two modes of operation are suitable for an unbalanced type of data transfer between one primary and the other secondary stations whereas the third one is suitable for a balanced type of data transfer.

Normal Response Mode (NRM) :

This mode is suitable for point-to-point as well as point-to-multipoint configurations. Here the primary station will control the overall data link management. It is a synchronous mode of communication.

Asynchronous Response Mode (ARM) :

- This mode is used for communication between primary and secondary stations. As the name indicates it is an asynchronous mode of communication.
- In ARM the secondary station can transmit response (frame) without taking permission from the primary station.

Scanned by CamScanner

- This is not allowed in NRM. Therefore NRM is a more disciplined mode than ARM. The responsibility of link management function still lies with the primary station.

Asynchronous Balanced Mode (ABM) :

- This mode is applicable to the point to point communication between two combined station.
- As both these stations are combined stations, they are capable of link management functions.
- As the communication is asynchronous, one station can transmit a frame without permission from the other station. In this mode information frames can be transmitted in full duplex manner.

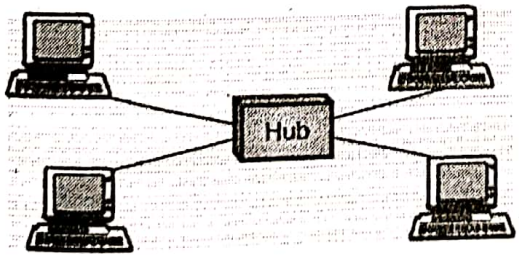
Chapter 4 : Medium Access Control Layer & LAN [Total Marks – 15]

Q. 2 (b) Explain repeater, hub, bridge, switch, gateway. (15 Marks)

Ans. :

Hubs :

- The general meaning of the word hub is any connecting device. But its specific meaning is multiport repeater.
- It is normally used for connecting stations in a physical star topology.
- All networks require a central location to connect various segments of media coming from various nodes.
- Such a central location is called as a hub. A hub organises the cables and relays signals to the other media segments as shown in Fig. 1-Q. 2(b).
- There are three main types of hubs :
  1. Passive hubs 2. Active hubs 3. Intelligent hubs



(G-350) **Fig. 1-Q. 2(b) : Hub**

Repeaters :

- A repeater is a connecting device which can operate only in the physical layer.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are called repeaters.
- A repeater receives a signal and before it gets attenuated or corrupted, regenerates the original signal.
- Thus we can use a repeater to extend the physical length of LAN .
- Repeater is not an amplifier because amplifiers simply amplify the entire incoming signal along with noise.
- Signal – regenerating repeaters create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it and retransmitting only the desired information.
- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.
- Repeaters operate at the physical layer of the OSI model and they deal with the actual physical signals.

Gateways :

- When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a gateway is used.
- A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks.
- Gateways comprise of software, dedicated hardware or a combination of both. Gateway operate through all the seven layers of the OSI model and all five layers of the internet model.
- A gateway can actually convert data so that it works with an application on a computer on the other side of the gateway. For e.g. a gateway can receive e-mail message in one format and convert them into another format.
- Gateways can connect systems with different communication protocols, languages and architecture. For e.g. IBM networks using Systems Network Architecture (SNA) can be connected to LANs using a gateway.

Switches :

- A switch is a device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in a LAN.
- The switch has a buffer for each link to which it is connected. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.

Scanned by CamScanner

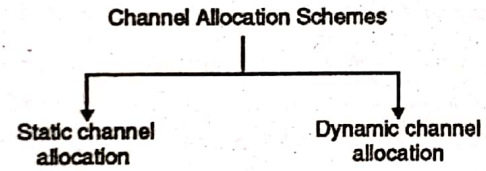
- If the outgoing link is free, the switch sends the frame to that particular link.
- Switches are of two types :
  1. Store - and - forward switch
  2. Cut - through switch.
- A store - and - forward switch stores the frame in the input buffer until the whole packet has arrived.
- A cut-through switch, forwards the packet to the output buffer as soon as the destination address is received.

Q. 5 (a) Explain channel allocation problem. Explain CSMA / CD protocol. A network with CSMA / CD has 10 Mbps bandwidth and 25.6 mS maximum propagation delay. What is the minimum frame size ? (10 Marks)

Ans. :

The channel allocation problem :

- In a broadcast network, the single communication channel is to be allocated to one transmitting user at a time. The other users connected to this medium should wait.
- This is called as channel allocation. There are two different schemes used for channel allocation as shown in Fig. 1-Q. 5(a) .



(G-266) **Fig. 1-Q. 5(a)**

Static channel allocation in LANs and MANs :

- The traditional way of allocating a single channel, among many users is by means of frequency division multiplexing (FDM).
- The Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are the examples of static channel allocation.
- In these methods either a fixed frequency band or a fixed time slot is allotted to each user. Thus either the entire available bandwidth or entire time is shared.
- The problem in these methods is that if all the N number of users are not using the channel the channel bandwidth is wasted and if there are more than N users who want to use the channel they cannot do so for the lack of bandwidth.
- For a small number or users and light traffic the static FDM is an efficient method of allocation but its performance is poor for large number of users, bursty and heavy traffic etc.
- The static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used, for computer networks where the traffic is of bursty nature.
- To see the poor performance of static channel, Consider an example for FDM system where the mean time delay (T) for a channel of capacity C bps, with an arrival rate of λ frames/sec.
- Each frame having a length drawn from an exponential probability density function with mean $1/\mu$ bits/frame is given as,

$$T = \frac{1}{\mu C - \lambda}$$

- If the single channel is divided into N independent subchannels the above equation is modified as follows :

$$T_{FDM} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda}$$

$$T_{FDM} = NT$$

- From the above equation, it is clear that the mean delay using FDM is worse. The static channel allocation has a poor performance with bursty traffic and hence generally dynamic channel allocation is used, for computer networks where the traffic is of bursty nature.

Dynamic channel allocation :

In this method either a fixed frequency or fixed time slot is not allotted to the user. The user can use the single channel as per his requirement. Following assumptions are made for the implementation of this method :

1. Station model – This model consists of N independent stations such as a PC, computer etc. which can generate frames for transmission.
2. Single channel – A single channel is available for all communication.
3. Collision – If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting signal is garbled. This is called as collision.
4. Continuous or slotted time – There is no master clock used to divide time into discrete time intervals. So frames can begin at any random instant. This is continuous time. For a slotted time, the time is divided into discrete time slots.
5. Carrier or No carrier sense – Stations sense the channel before transmission or they directly transmit without sensing the channel.

Scanned by CamScanner

Solution to example :

Given : CSMA / CD, BW = 10 Mbps, Maximum propagation delay $T_P = 25.6$ μsec.

To find : Minimum frame size.

- The time required for the signal to propagate between the two farthest stations be T_P.
- With CSMA / CD, in the worst case, a station needs to transmit for a period of 2 T_P to detect the collision.
- To make CSMA / CD work, it must be ensured that the minimum frame size is equal to 2 T_P.

$$\therefore \text{ Minimum frame size } = 2T_P = 51.2\ \mu S.$$

$$\text{But BW } = 10 \times 10^6 \text{ bits/sec.}$$

$$\therefore 1 \text{ sec} \equiv 10^7 \text{ bits}$$

Then 51.2 μS ≡ ?

$$\therefore \frac{1}{51.2 \times 10^{-6}} = \frac{10^7}{x}$$

$$\therefore x = 51.2 \times 10^{-6} \times 10^7$$

$$= 512 \text{ bits}$$

∴ Minimum frame size = x = 512 bits or 64 bytes

Chapter 5 : Network Layer [Total Marks - 45]

Q. 3 (b) Describe IPv4 header format with diagram. **(10 Marks)**

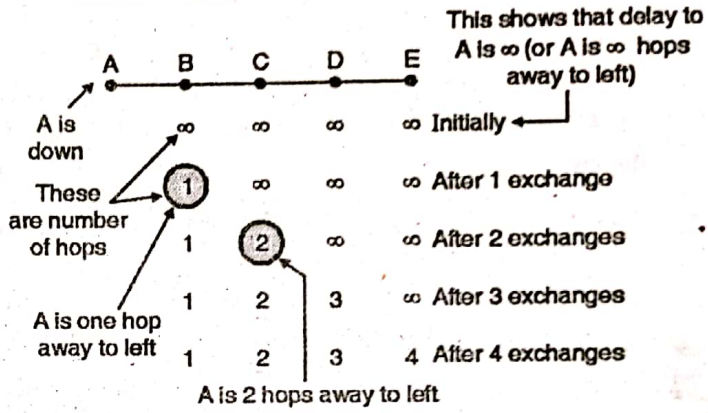
Ans. : Please Refer Q. 2(b) of Dec. 2018.

Q. 4 (b) Explain distance vector routing protocol. What is count to identify problem How to overcome it ? **(10 Marks)**

Ans. : Distance Vector Routing Algorithm : Please refer Q. 6(b) of Dec. 2018.

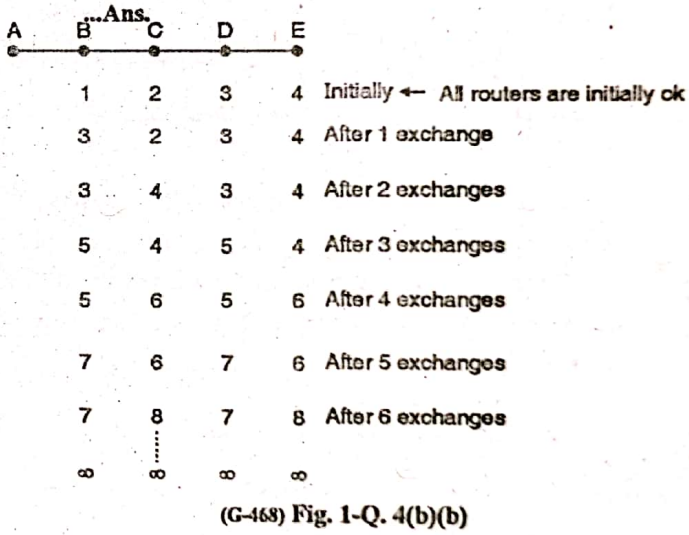
Count to Infinity problem :

- Consider a linear subnet of Fig. 1-Q. 4(b) which has five nodes. The delay metric used is the number of hops.
- Assume that A is initially down and that all the other routers know this. So all the routers have recorded that the delay to A is infinity.
- When A becomes OK, the other routers come to know about it via the vector exchanges. Then suddenly a vector exchange at all the routers will take place simultaneously.
- At the time of first vector exchange, B comes to know that its left neighbour has a zero delay to A. So as shown in Fig. 1-Q. 4(b)(a). B makes an entry in its routing table that A is one hop away to the left.
- All the other routers still think that A is down. So in the second row of Fig. 1-Q. 4(b)(a), the entries below C D E are ∞.
- On the second vector exchange, C comes to know that B has a path of 1 hop length to A, so C updates its routing table and indicates a path of 2 hop length. But D and E do not change their table entries.



(G-467) Fig. 1-Q. 4(b)(a)

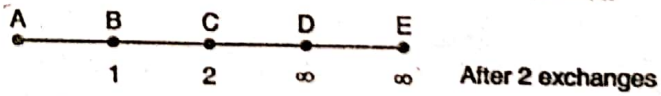
...Ans.



(G-468) Fig. 1-Q. 4(b)(b)

- So after the second vector exchange the entries in the third row of Fig. 1-Q. 4(b)(a) are :

(G-468(a))

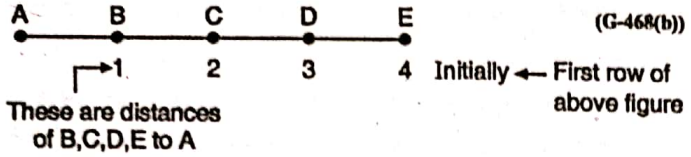


- Similarly D and E will update their routing tables after 3 and 4 exchanges respectively.
- So we conclude that the good news of A has recovered has spread at a rate of one hop per exchange.

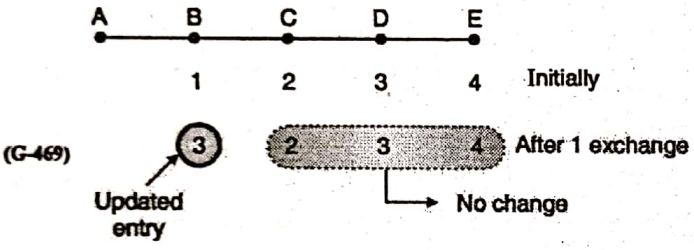
Explanation of Fig. 1-Q. 4(b)(b) :

- Now refer Fig. 1-Q. 4(b)(b). Here initially all routers are OK. The routers B, C, D and E have distances of 1, 2, 3 and 4 respectively to A. So the first row of Fig. 1-Q. 4(b)(b) is as follows :

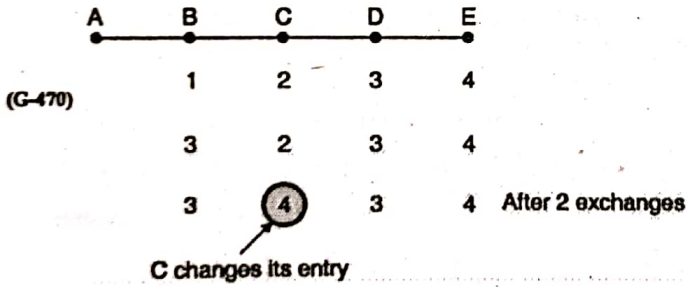
Scanned by CamScanner



- Now imagine that suddenly A goes down or line between A and B is cut.
- At the first packet exchange B does not hear anything from A (because A is down). But C says "I have a path of length 2 to A". But poor B does not understand that this path is through B itself.
- So B thinks that it can reach A via C with a path length 3. (B to C 1 hop and C to A 2 hops) so it accordingly updates its routing table. But D and E do not update their entries. So the second row of Fig. 1-Q. 4(b)(b) looks as follows :



- On the second exchange C realizes that both its neighbours (B and D) claim to have a path of length 3 to A. So it picks one of them at random and makes its new distance to A as 4. This is shown in row 3 of Fig. 1-Q. 4(b)(b). It is repeated below.



- Similarly the other routers keep updating their tables after every exchange.
- It is expected that finally we should get ∞ in the router tables of B, C, D and E indicating that A is down. We do reach this state at the end in Fig. 1-Q. 4(b)(b) but after a very long time.
- The conclusion is bad news propagates slowly. This problem is called as **count-to-infinity** problem.
- The solution to this problem is to use the split horizon algorithm.

Split horizon algorithm :

- To avoid the count to infinity problem, several changes in the algorithm have been suggested. But none of them work satisfactorily in all situations.
- One particular method which is widely implemented, is called as the **split horizon algorithm.**
- In this algorithm, the minimum cost to a given destination is not sent to a neighbour if the neighbour is the next node along the shortest path.
- For example if node A thinks that the best route to node B is via node C, then node A should not send the corresponding minimum cost to node C.

Q. 5 (b) Explain congestion control. Explain leaky bucket algorithm. (10 Marks)

Ans. : Leaky Bucket Algorithm : Please refer Q. 3(b) of Dec. 2018.

Need of congestion control :

It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.Congestion will result in long queues, which results in buffer overflow and loss of packets.So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

Q. 6 (b) Short note on Network Address Translation (NAT). (5 Marks)

Ans. :

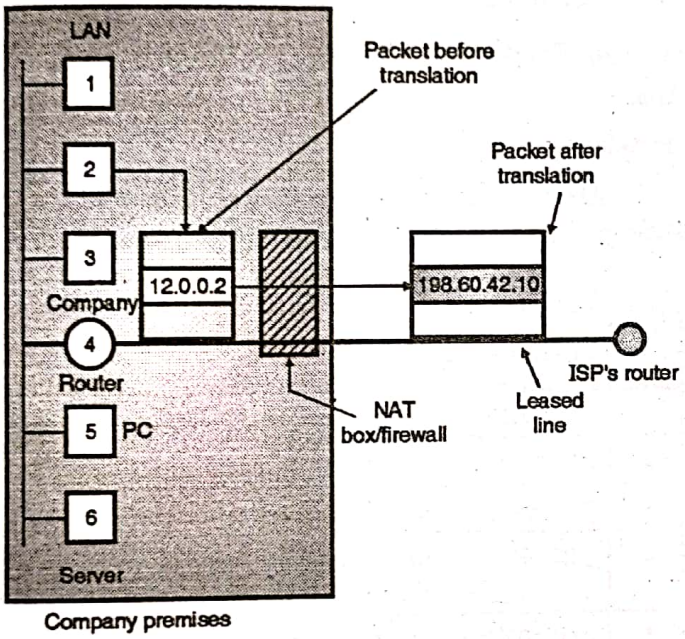
NAT – Network Address Translation :

- The basic idea in NAT is that each company is assigned a single IP address or at the most a small number of IP addresses so as to access the Internet.
- Within the company, every computer gets a unique IP address which is used for routing the internal traffic of the office.
- But when a packet goes out of the company, and goes to ISP, the translation of IP address takes place there.
- In order to make this scheme work, three ranges of IP addresses have been declared as private. Companies can use these addresses internally as per their requirement. However no packet containing these addresses is allowed to appear on the Internet. The three reserved ranges are as follows :

Range 1	10.0.0.0 to 10.255.255.255/8	16777216 Hosts
Range 2	172.16.0.0 to 173.31.255.255/12	1048 576 Hosts
Range 3	192.168.0.0 to 192.168.255.255/16	65 536 Hosts

Scanned by CamScanner

- Generally most companies choose the addresses from the first range.
- Refer Fig. 1-Q. 6(b) which explains the operation of NAT. It shows that within the company premises, every machine has a unique address of the form 12.a.b.c.
- But when a packet leaves the company premises, it passes through the NAT box. This box converts the internal IP address 12.0.0.2 in Fig. 1-Q. 6(b) to the company's true IP address 198.60.42.10.
- The NAT box is generally combined with a firewall. It is also possible to integrate the NAT box into company's router.



(G-551) Fig. 1-Q. 6(b) : NAT

Q. 6 (d) Short note on : ARP. (5 Marks)

Ans. : Please refer Q. 6(c) of Dec. 2018.

Q. 6 (e) Short note on : ICMP. (5 Marks)

Ans. : Please refer Q. 4(a) of Dec. 2018.

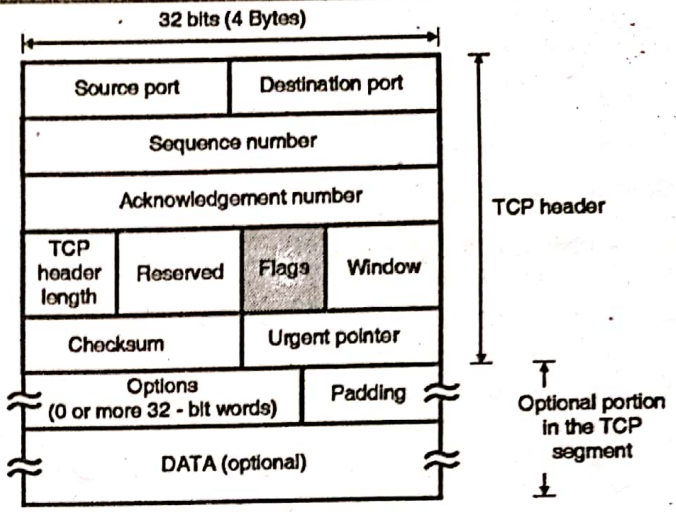
Chapter 6 : Transport Layer [Total Marks - 15]

Q. 2 (c) Describe TCP header with diagram. (10 Marks)

Ans. :

The TCP segment header :

Fig. 1-Q. 2(c) shows the layout of a TCP segment. Every segment begins with a 20 byte fixed format header.



(G-611) Fig. 1-Q. 2(c) : TCP header format

- The fixed header may be followed by header options.
- After the options, if any, upto 65535 – 20 – 20 = 65495 data bytes may follow. Note that the first 20 bytes correspond to the IP header and the next 20 correspond to the TCP header.
- The TCP segment without data are used for sending the acknowledgements and control messages.

Source port :

A 16-bit number identifying the application the TCP segment originated from within the sending host. The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49,151) and private ports (49,152 through 65,535). Port assignments are used by TCP as an interface to the application layer.

Destination port :

A 16-bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports.

Sequence number :

A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection. After reaching $2^{32} - 1$, this number will wrap around to 0.

Acknowledgement number :

A 32-bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on.

Header length or offset :

A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer). Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes. This field is required because the size of the options field(s) cannot be determined in advance. Note

Scanned by CamScanner

that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

Reserved :

A 6-bit field currently unused and reserved for future use.

Control bits or flags :

1. **Urgent pointer (URG) :** If this bit field is set, the receiving TCP should interpret the urgent pointer field.
2. **Acknowledgement (ACK) :** If this bit field is set, the acknowledgement field is valid.
3. **Push function (PSH) :** If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible. An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.
4. **Reset the connection (RST) :** If this bit is present, it signals the receiver that the sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinquished.
5. **Synchronize (SYN) :** When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.
6. **No more data from sender (FIN) :** If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window :

A 16-bit integer used by TCP for flow control in the form of a data transmission window size. This number tells the sender how much data the receiver is willing to accept. The maximum value for this field would limit the window size to 65,535 bytes, however a "window scale" option can be used to make use of even larger windows.

Checksum :

A TCP sender computes a value based on the contents of the TCP header and data fields. This 16-bit value will be compared with the value the receiver generates using the same computation. If the values match, the receiver can be very confident that the segment arrived intact.

Urgent pointer :

In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible. This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options :

In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver. Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits). The most common option is the Maximum Segment Size (MSS) option. A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option. Other options are often used for various flow control and congestion control techniques.

Padding :

Because options may vary in size, it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32-bit word boundary as defined by the standard.

Data :

Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header fields constitutes a TCP segment.

Q. 6 (c) Short note on Berkeley sockets. (5 Marks)

Ans. :

Berkeley sockets :

Table 1-Q. 6(c) lists various transport primitives used in Berkeley UNIX for TCP.

Table 1-Q. 6(c)

Sr. No.	Primitive	Meaning
1.	SOCKET	Create a new communication end point.
2.	BIND	Provide a local address to a socket
3.	LISTEN	Show willingness to accept connections
4.	ACCEPT	Block the caller as long as a connection attempt does not arrive
5.	CONNECT	Attempt to establish a connection
6.	SEND	Send data
7.	RECEIVE	Receive data
8.	CLOSE	Release the connection

- The first four primitives in the Table 1-Q. 6(c) are executed in the same order by the server.
- The SOCKET primitive creates a new end point and allocates table space for it within the transport entity.
- The newly created sockets do not have addresses. These are assigned using the BIND primitive.
- The LISTEN primitive allocates space to queue the incoming calls in case if several clients wish to connect at the same time.
- To block waiting for an incoming connection, the server executes an ACCEPT primitive. When a TPDU requesting for a connection arrives, the transport entity creates a new socket and returns a file descriptor for it.

Scanned by CamScanner

- These were the primitives corresponding to server side. Now consider the client side.
- On the client side also a socket needs to be created first using the SOCKET primitive, however the BIND is not required.
- The CONNECT primitive blocks the caller and initiates the connection process.
- When it completes (which is indicated by an appropriate TPDU received from the server), the client process is unblocked and the connection is established.
- After this both the sides can use SEND and RECEIVE primitives to send and receive data.
- In order to release the connection, both sides have to execute a CLOSE primitive.

Chapter 7 : Application Layer
[Total Marks - 10]

Q. 6 (f) Short note on DNS. (5 Marks)

Ans. :

Domain name system (DNS) :

- For communication to take place successfully, the sender and receiver both should have addresses and they should be known to each other.
- The addressing in application program is different from that in the other layers. Each program will have its own address format. For example an e-mail address is like sachinshaha@vsnl.net where as the address to access a web page is like http :// www.google.com/
- It is important to note that there is an alias name for the address of remote host. The application program uses an alias name instead of an IP address.
- This type of address is very convenient for the human beings to remember and use. But it is not suitable for the IP protocol.
- So the alias address has to be mapped to the IP address. For this an application program needs service of another entity.
- This entity is an application program called DNS. Note that DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

How does DNS work ?

- To map a name onto an IP address, an application program calls a library procedure called the **resolver.** The name is passed on to the resolver as a parameter.
- The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver.
- The resolver then sends this address to the caller. Then the program can establish a TCP connection with the destination or sends in the UDP packets.

Q. 6 (g) Short note on : SMTP (5 Marks)

Ans. : Please refer Q. 6 (d) of Dec. 2018.

□□□

Scanned by CamScanner

Question Papers

Dec. 2018

Q. 1 Any – 5 **(20 Marks)**

(a) What are the design issues for the OSI layers ?

(b) Differentiate between connection oriented and connectionless service ?

(c) List the advantages of fiber optics as a communication medium.

(d) Explain with examples the classification of IPv4 addresses.

(e) Explain in short different framing methods.

(f) Explain the need of subnet mask in subnetting.

Q. 2 (a) What is topology ? Explain the types of topologies with diagram, advantages and disadvantages. **(10 Marks)**

(b) What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(10 Marks)**

Q. 3 (a) Explain CSMA protocols. Explain how collision are handled in CSMA / CD. **(10 Marks)**

(b) What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(10 Marks)**

Q. 4 (a) What is ICMP protocol ? Explain the ICMP header format with diagram. **(10 Marks)**

(b) Write a program for client server application using Socked Programming (UDP). **(10 Marks)**

Q. 5 (a) Explain the use of TCP timers in detail. **(10 Marks)**

(b) Compare open loop congestion control and closed loop congestion control. **(10 Marks)**

Q. 6 Write a short note on the following (Any Two) : **(20 Marks)**

(a) Internetworking Devices

(b) Distance Vector Routing

(c) ARP / RARP

(d) SMTP

□□□

May 2019

Q. 1 (a) Explain design issues of layers. Explain ISO OSI reference model with diagram. **(10 Marks)**

(b) Explain design issues of Data Link layer. Explain Sliding Window protocol Selective Repeat. **(10 Marks)**

Q. 2 (a) Explain with diagram the relationship between Protocol, Interface and Service. **(5 Marks)**

(b) Explain Repeater, Hub, Bridge, Switch, Gateway. **(5 Marks)**

(c) Describe TCP header with diagram. **(10 Marks)**

Q. 3 (a) Explain different framing methods. What are the advantages of variable length frame over fixed layer frame ? **(10 Marks)**

(b) Describe IPv4 header format with diagram. **(10 Marks)**

Q. 4 (a) Classify transmission media and compare them. **(10 Marks)**

(b) Explain distance vector routing protocol. What is count to identify problem How to overcome it ? **(10 Marks)**

Q. 5 (a) Explain channel allocation problem. Explain CSMA / CD protocol. A network with CSMA / CD has 10 Mbps bandwidth and 25.6 mS maximum propagation delay. What is the minimum frame size ? **(10 Marks)**

(b) Explain congestion control. Explain leaky bucket algorithm. **(10 Marks)**

Q. 6 Short note on (Any 4) : **(20 Marks)**

(a) HDLC.

(b) Network Address Translation (NAT).

(c) Berkeley Sockets.

(d) ARP.

(e) ICMP.

(f) DNS.

(g) SMTP.

Scanned by CamScanner

Your Success is Our Goal

Semester V - Computer Engineering

- **Computer Networks**
- **Database Management System**
- **MICROPROCESSOR**
- **Theory of Computer Science**
- **Multimedia System (Dept. Elective I)**
- **Advance Operating System (Dept. Elective I)**

es® easy-solutions now with TechKnowledge™ Publications

Paper Solutions Trusted by lakhs of students from more than 15 years

Distributors

MUMBAI

Student's Agencies (I) Pvt. Ltd.
102, Konark Shram, Ground Floor, Behind Everest Building,156 Tardeo Road, Mumbai.
M :℡91672 90777.

Vidyarthi Sales Agencies
Shop. No. 5, Hendre Mansion, Khotachiwadi,157/159, J.S.S Road, Girgaum, Mumbai. M :℡98197 76110.

Bharat Sales Agency
Goregaonkar Lane, Behind Central Plaza Cinema, Charni Road, Mumbai. M :℡86572 92797

Ved Book Distributors - Mr. Sachin Waingade
(For Library Orders)
M : 80975 71421 / 92208 77214.
E : mumbai@techknowledgebooks.com

EMO45A Price ₹ 75/-

BOOKS ARE AVAILABLE AT ALL LEADING BOOKSELLERS !!

B-50

Scanned by CamScanner